Div 760

NBSIR 81-2207 (R)

The Role of Behavioral Science in Physical Security Proceedings of the Fourth Annual Symposium, July 25-26, 1979

edited by
George M. Lapinsky
Ann Ramey-Smith
Center for Consumer Product Technology
and Stephen T. Margulis
Center for Building Technology
U.S. Department of Commerce
National Bureau of Standards
Washington, DC 20234

February 1981

This work was supported by the Defense Nuclear Agency,
Robert R. Monroe, Vice Admiral, USN, Director
under Subtask Code B99QAXRA101, Work Unit Code 08

Distribution Statement: This publication is required for official use or for administrative or operational purposes only. Distribution is limited to U.S. Government agencies. Other requests for this document must be referred to the Director, Defense Nuclear Agency, Attn: SONS, Washington, DC 20305.

sponsored by the
Law Enforcement Standards Laboratory
and the
Consumer Sciences Division
National Bureau of Standards
Washington, DC 20234
and the
Nuclear Surety Directorate
Defense Nuclear Agency
Washington, DC 20305

ERRATA

The following sentence should be inserted on page 71, first paragraph, after the third sentence:

> The second is to evaluate the effectiveness of measures which are aimed at deterring, detecting, and defeating these threats.

NBSIR 81-2207 (R)

THE ROLE OF BEHAVIORAL SCIENCE IN PHYSICAL SECURITY PROCEEDINGS OF THE FOURTH ANNUAL SYMPOSIUM, JULY 25-26, 1979

edited by
George M. Lapinsky
Ann Ramey-Smith
Center for Consumer Product Technology
and Stephen T. Margulis
Center for Building Technology
U.S. Department of Commerce
National Bureau of Standards
Washington, DC 20234

February 1981

This work was supported by the Defense Nuclear Agency,
Robert R. Monroe, Vice Admiral, USN, Director
under Subtask Code B99QAXRA101, Work Unit Code 08

sponsored by the
Law Enforcement Standards Laboratory
and the
Consumer Sciences Division
National Bureau of Standards
Washington, DC 20234
and the
Nuclear Surety Directorate
Defense Nuclear Agency
Washington, DC 20305

U.S. DEPARTMENT OF COMMERCE, Malcolm Baldrige, *Secretary*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

ACKNOWLEDGMENTS

The Fourth Annual Symposium on the Role of Behavioral Science in Physical Security was organized and developed by Mr. Marvin Beasley, Nuclear Surety Directorate of the Defense Nuclear Agency, with the joint sponsorship of the Law Enforcement Standards Laboratory (LESL) and the Consumer Sciences Division, both of the National Bureau of Standards. This document was physically prepared and reviewed by LESL, under the direction of Lawrence K. Eliason, Chief.

CONTENTS

Page

Preface iv
Foreword v
Abstract vi

Formal Presentations (First Day) 1

Welcoming Remarks
Major General Richard N. Cody 3

Introductions
LTC Donald R. Richards 5

Security Performance Measurement Methodology
Dr. Robert Hall 7

Security Force Selection and Training
Dr. Preston Abbott and Dr. Richard Orth 19

Standard Ergonomics Reference Data Systems (SERDS)
Dr. Harold P. Van Cott and Mr. Joel J. Kramer 29

Status Report on the NBS Vigilance Research Project
Dr. John V. Fechter 33

Psychological Deterrents to Nuclear Theft
Clare Goodman and George Lapinsky 39

Organization and Mission of the USAF Human Resources Laboratory
Dr. Jeffrey E. Kantor 45

Behavioral Research for U.S. Air Forces - Europe
Mr. Hendrick Ruck 51

Behavioral Impact on Shipboard Security
Mr. William Stinson 57

Behavioral Model of Shipboard Physical Security--Contractor Support
Mr. William Stinson 61

Measures of Effectiveness for Shipboard Security
Mr. John Evans and Mr. John F. Haben 67

Use of Analogous Incidents in Characterizing Threats to Nuclear Safeguards
Mr. Richard S. Schechter and Prof. John M. Heineke. 71

Monomolecular Atmospheric Ion Levels
Dr. Charles Wallach 77

Discussion (Second Day) 79

Panel Discussion of Selected Presentations 81

Attendees' Round Table Discussion: Comments and Opinions on Current Behavioral Research and Future Needs 89

List of Attendee's 91

PREFACE

These proceedings are the result of a symposium, the fourth of a series, held on July 25-26,]979, at the Defense Nuclear Agency, Alexandria, VA. The purpose of the symposium was to continue defining the contributions that behavioral science can make to enhance physical security systems.

The symposium was jointly sponsored by the Law Enforcement Standards Laboratory (LESL), the Consumer Sciences Division of the National Bureau of Standards (NBS) and the Nuclear Surety Directorate of the Defense Nuclear Agency. Approximately 60 delegates from both Government and industry attended the symposium.

The editors wish to acknowledge the cooperation of the Defense Nuclear Agency staff, particularly Major General Richard N. Cody, LTC Donald R. Richards, and Mr. Marvin Beasley. Appreciation is also extended to Ms. Addie Stewart and Ms. Barbara Stanton of the National Bureau of Standards for their assistance in preparing these proceedings.

George W. Lapinsky
Steve T. Margulis
Ann M. Ramey-Smith
(Editors)

FOREWORD

The Defense Nuclear Agency (DNA) is engaged in a continuing effort to enhance the security of nuclear weapons storage. In this effort, it is receiving technical support from the National Bureau of Standards' Law Enforcement Standards Laboratory (LESL), whose overall program involves the application of science and technology to the problems of crime prevention, law enforcement and criminal justice.

LESL is assisting DNA's physical security program with support in the behavioral science, the chemical science and the ballistic materials areas, among others.

Among the tasks being performed by LESL for DNA are the preparation and publication of several series of technical reports on the results of its researches. This document is one such report.

Technical comments and suggestions are invited from all interested parties. They may be addressed to the authors,* the editors, or the Law Enforcement Standards Laboratory, National Bureau of Standards, Washington, DC 20234.

Lawrence K. Eliason, Chief
Law Enforcement Standards Laboratory

*Points of view or opinions expressed in this volume are those of the individuals to whom they are ascribed, and do not necessarily reflect the official positions of either the National Bureau of Standards or the Defense Nuclear Agency.

ABSTRACT

This document contains the proceedings of the fourth annual symposium on "The Role of Behavioral Science in Physical Security," held on July 25-26, 1979. The symposium provided a forum for presenting and discussing current behavioral science contributions to physical security. Generally, attendance was limited to key personnel in the services, other Government Agencies, and private firms currently on contract with the Defense Nuclear Agency. Papers were presented on the first day, followed by a discussion session the second day.

Key words: Behavioral science; collusion; ergonomics; human factors; performance; personnel selection; physical security; psychological deterrents; threat analysis; training; vigilance.

Formal Presentations (First Day)

WELCOMING REMARKS

Major General Richard N. Cody
U.S. Air Force
Deputy Director, Operations and Administration
Defense Nuclear Agency, Washington, DC 20305

We, in DNA, are extremely pleased to co-sponsor, with the National Bureau of Standards, this fourth workshop on the role of behavioral science in physical security. I am particularly happy to have the Undersecretary for Defense, Research, and Engineering (USDRE) Physical Security Action Group and representatives from both DOE and NRC, here to participate in this effort.

DNA is vitally interested in the effects of human behavior on all types of security functions. We have every reason to expect that you perceive our security problems with empathy and concern, and that you will help us to work toward their solution. We are very proud of our past efforts, which place us, along with some of you, in the category of pioneers in applying the behavioral sciences to security problems.

This is the fourth meeting held to discuss behavioral science and DNA's nuclear security mission. We feel that DNA has made considerable progress with the initiation of several funded research projects to examine human performance in security systems. This limited-attendance meeting is a means of updating the Physical Security Equipment Action Group (PSEAG) and other interested observers on current status of behavioral research in the nuclear security community. Additionally, tomorrow we will be looking to some of the DOD behavioral scientists for long-term participation in an advisory role with our program managers. We feel this symposium is a turning point for DNA's behavioral research program.

We have two distinguished gentlemen who will speak to you about what we have been doing here and what they have been doing to help us. These two gentlemen have independently visited a number of our nuclear weapons installations to observe the performance of security personnel. Their data, although preliminary and, as they will explain to you, sensitive in nature, indicate that our desire to examine human behavior and the human factors involved with security is well justified. Further, the data that we will be gathering will assist in the formulation of a program plan which will more realistically balance applied research against theoretical research.

During fiscal year 1980, DNA looks forward to the completion of our initial efforts and the development of a definitive behavioral research program. We must have personnel data that supports other DNA efforts. Most notable is the development of a conceptual, integrated security system for the 1990's. Without a strong human factors effort, the system cannot be truly considered "integrated." DNA's commitment to this position has not diminished, in fact, it has been strengthened. I want to thank you again for coming to help my staff in their efforts to develop a more effective nuclear security program through the application of behavioral sciences.

INTRODUCTIONS

LTC Donald R. Richards
U.S. Army
Chief, Nuclear Security Division
Defense Nuclear Agency, Washington, DC 20305

The DNA commitment to behavioral science, and that I perceive among the Services as well, is continuing to grow stronger. The work to implement the current upgrade program in Europe, which has many severe problems, serves to further emphasize the requirements in the behavioral science area. As we work toward development of our Conceptual Integrated Security System, it becomes increasingly evident that we must pay close attention to human factors.

This is a limited attendance group. We selected you specifically from the larger groups that we had the previous years. We did that purposely, because we wanted to have the more concentrated effort that you can have with a smaller group, with a little more interplay. Especially tomorrow, for it is going to be critically important to us to get some feedback from all of you with respect to what you think we should be doing in addition to the directions that we are now taking. Something that you are aware of, as are we, is that when working with an integrated security system, you can have the best hardware in the world and the best policies, but if you do not take into consideration how people live, work, and interact with the hardware you are not going to have an integrated security system. We are hoping to get from you your candid and constructive comments on the program as it is now and as we hope it will be in the future.

SECURITY PERFORMANCE MEASUREMENT METHODOLOGY

Dr. Robert Hall
Mission Research Corporation, Alexandria, VA 22312

The purpose of this talk is to report on a behavioral research program that conducted a series of detailed interviews with military security personnel. The objective has been to assess the job perceptions of security personnel, to identify performance problems, and determine what aspects of those problems one determined by the nature of the job.

At the last symposium, it was suggested that the behaviorists should get out from behind their desks and find out what is going on out at the site. The present effort is an attempt to accomplish this.

Phase I began, like many studies, with a literature search. I will only pause to say that the literature search was disappointing. When we did a review of the articles that were selected from the literature and a computer search of available technical abstracts, we found that a very small percentage of the documents could be used to make decisions about security personnel policies, or the interaction of personnel and equipment. We found many behavioral documents that had potential implications, but when evaluated by a fairly rigorous selection criterion, we were disappointed by the amount of usable information that was in the literature.

The next step was to visit two Air Force and one Army site. During these visits we constructed and tested questions and topics; we evaluated the data and issues raised by the questions and we identified a set of problems which were manifested in the final set of data.

Phase II involved the testing and implementation of structured interview techniques and data collection at the U.S. Army CONUS sites. The data have been tabulated and analyzed, and we are presenting some of the conclusions and recommendations from that data here today. I want to emphasize that I am only presenting selected issues and a very small portion of the data we have available.

The data collection instruments included structured interviews with enlisted security personnel below E5, security managers (above E5) and an inventory of site characteristics. Most of the data I will be talking about was obtained from security personnel below the rank of E5. Interviews were conducted at the Army CONUS sites on a 24-hr basis under operational conditions. The data were evenly collected over a period of 8 to 10 d to make certain that we had included all three shifts, rotations, and weekends.

The second data collection instrument was the Security Manager's Interview Schedule. This instrument was designed for people of E5 and above (the platoon sergeant, the first and second lieutenants, and the captain of the company). The Security Manager's Interview data have parallel questions, that make it possible to contrast their particular view of what is wrong with that of the troops (below E5).

The Site Characterization Data Collection Schedule dealt with areas such as lighting, TV displays, and site peculiarities that could have an impact on an individual's performance.

The data reported here concerns the perceived environment, that is, the opinions, attitudes, and perceptions of other people, rather than controlled observations.

Reports of the perceived environment were organized under the following categories:

- career development
- job perceptions and attitudes
- peer group relationship
- vulnerability to intrusion
- performance reliability program
- inspections
- use of deadly force
- vigilance and readiness
- health and physical fitness
- personel problems
- training
- sensory capacities
- knowledge of terrain
- knowledge of sensors
- television assessment
- lighting
- environmental constraints
- communications
- response skills

The largest sample of data was collected on site and consists of 147 U.S. Army CONUS guards. A smaller sample of data was collected from interviews with 27 security managers at U.S. Army sites and during Phase I visits to U.S. Air Force sites.

Figure 1 addresses a question that was concerned with career objectives. The people were asked, "What are your career objectives?" The answers came from Army CONUS security personnel--below E5, most of whom are working out at the site. Law enforcement is their obvious career choice. When we look at security as a choice; only 5% said that they would reenlist in security.

Additional questions revealed that most of these people came into the Service expecting to acquire some law enforcement experience. They would sign up for white hat duty, Military Police, and were sadly disappointed. Often it was their opinion that they had been cheated by the enlistment officer and directed into a security job which they did not choose.

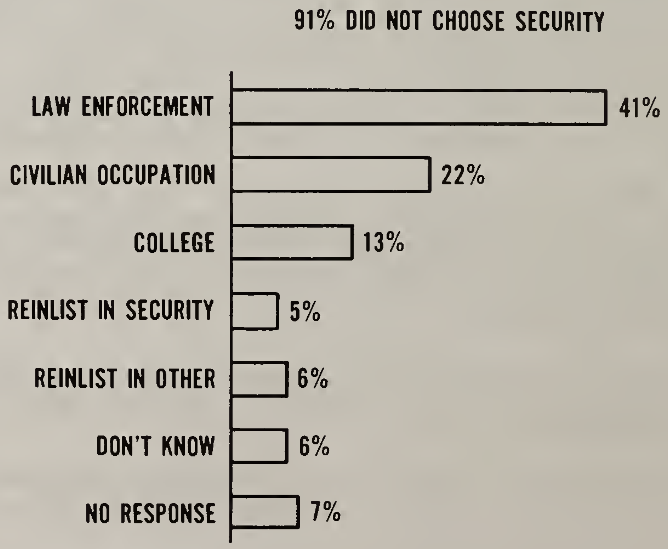

Figure 1. Career objectives.

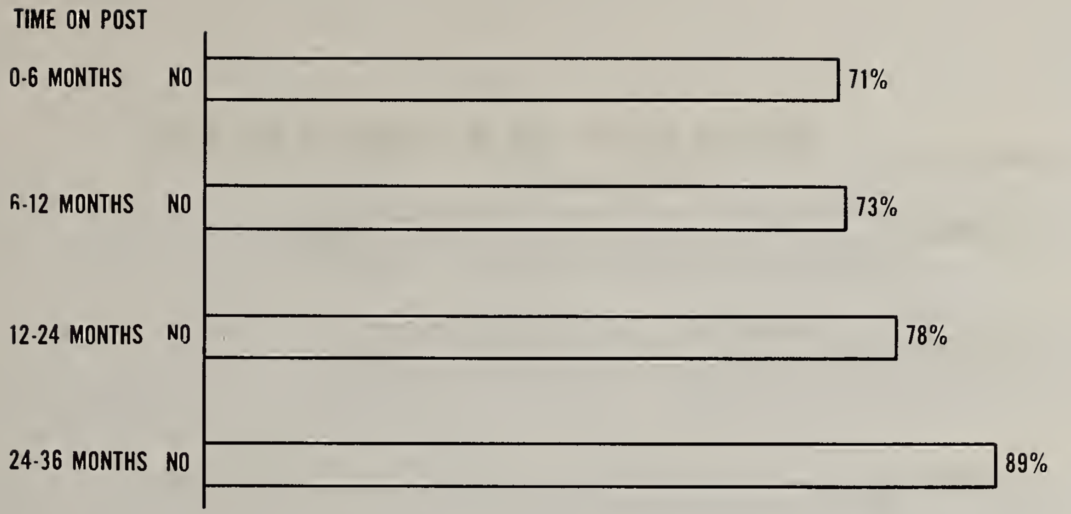

Figure 2. Percent of those who believe that the PRP does not select personnel properly (partitioned by time on post).

Regarding the Personnel Reliability Program (PRP), the question was asked, "Do you think the Personnel Reliability Program selects people properly?" In figure 2, we see that most of these people feel that the Personnel Reliability Program does not screen properly. The data in this figure have been partitioned by time on post.

MR. LEAHY: What was the question that they were asked?

DR. HALL: The question they were asked was, "Do you think the Personnel Reliability Program selects people properly?"

MR. STINSON: Selects people properly for careers? Or selects people properly for security? In other words, careers or security?

DR. HALL: For security duty.

MR. STINSON: Is there any way to differentiate between supervisors and actual security personnel?

DR. HALL: Yes, these are only data for security personnel. Any time it is managers' data, I will indicate it.

The data presented in figure 3 are the results of the question, "How would you describe your job?" Once again, these data indicate that the longer the personnel are on post the more likely they are to characterize the job as boring. Other related questions asked were: "Do you feel that you are treated fairly?" "Do you feel security personnel are treated fairly," and so forth. They all tend to show an increase in negative attitudes as a function of time on post.

The next topic concerned platoon loyalities (fig. 4). "Does your platoon support one another and stick together?" The answers, almost invariably, were "Yes." When asked, "How would you rank your platoon?", personnel tended

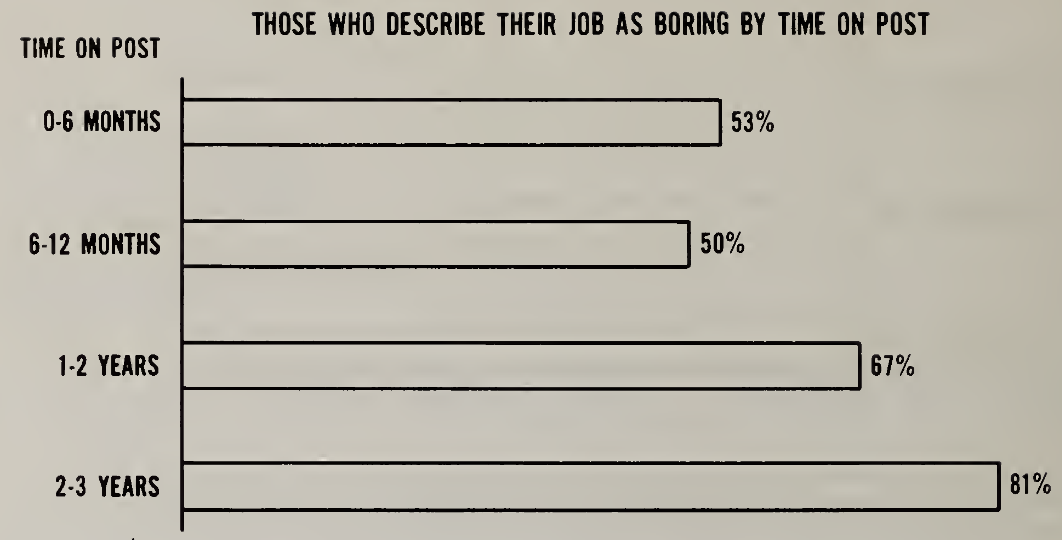

Figure 3. The job is boring.

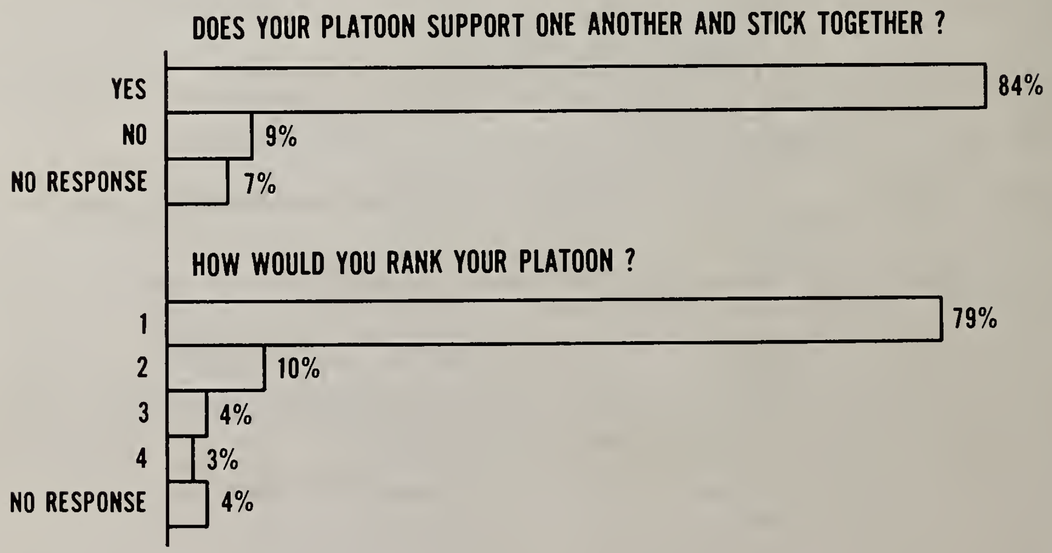

Figure 4. Platoon alliance (peer group relationships).

to rank their platoon as "number one." Within each platoon we found a good deal of competitive cohesiveness and esprit de corps. For example, it was reported that many of the problems of security personnel are handled at the platoon rather than the company level. There is active competition between platoons, and personnel are vocal about the "back office," or the company, being in conflict with the real needs of the people at the platoon level--people at the operational site.

Figure 5 shows the responses to the question, "What percent (of troops) could run a mile, fully equipped, and still perform their duties as a security guard?" We have two opinions expressed here. The top bar is the opinion of the operational personnel at the site; the bottom bar indicates the perception of the managers. We see an interesting divergence.

In order to ascertain perceived training needs, the question was asked, "How could training be improved?" (fig. 6). The most frequently occurring responses were: (1) realistic exercises, and (2) better instructors. A number of people were interested in terrorist training. It was the opinion of 5% that the training was adequate.

The question was asked, "Do you get adequate feedback concerning your performance in your job?" In figure 7 the positive and negative answers are summarized and plotted yes and no.

LTC RICHARDS: What is significant, is that the answers do not seem to change (as a function of time on post).

DR. HALL: This one does not change, as we might have expected it to look like the other attitudes that change as a function of time on post.

Figure 8 presents data from an instrumented Air Force site that has buried cable and fence disturbance sensors. The average number of alarms per day were plotted for the 10 worst days from the winter, spring, and summer quarters in order to show the true magnitude of the false alarm problem. Looking at the 10 worst days, one sees an almost unmanageable number of false alarms. In fact, we know that on the worst possible days, the alarms are so high that they are not recorded.

LTC RICHARDS: They have not turned the sensor system off yet, though.

DR. HALL: No. When it is not windy and the ground is not expanding and contracting, the system works well.

We asked a number of questions about electronic sensors and TV's and whether or not they felt these could be used as a substitute for the operator's performance. Figure 9 shows the responses to the question concerning TV's. "Do you feel TV can replace visual assessment?" These data are from a site that has perimeter TV and does not include the site that did not. So this data is from a sample of 99 security personnel. Seven percent said TV could replace visual assessment and 41% said it could not. Nineteen percent ranked it second to vision. Others listed a number of problems like "dead spots," "cannot see distinctly," and glare. We found that deployment of mobile cameras is something that is not checked. For example, there are no standard outside targets to indicate the cameras are deployed properly or that their resolution is adequate. In such situations it is not uncommon to find cameras looking at one another on the same sector of the perimeter while other sectors are not under TV surveillance. When the iris must be manually adjusted, for sunrise, and sunset (approximately 2 hr) the TV monitoring system is largely useless because these adjustments have not been made. Resolution targets are needed to evaluate the effects of weather on TV resolution. Problems of impaired visibility are common. We found, for example, a tower where plastic sun screens were so thick with smoke residue and dust that they obscured targets and degraded vision.

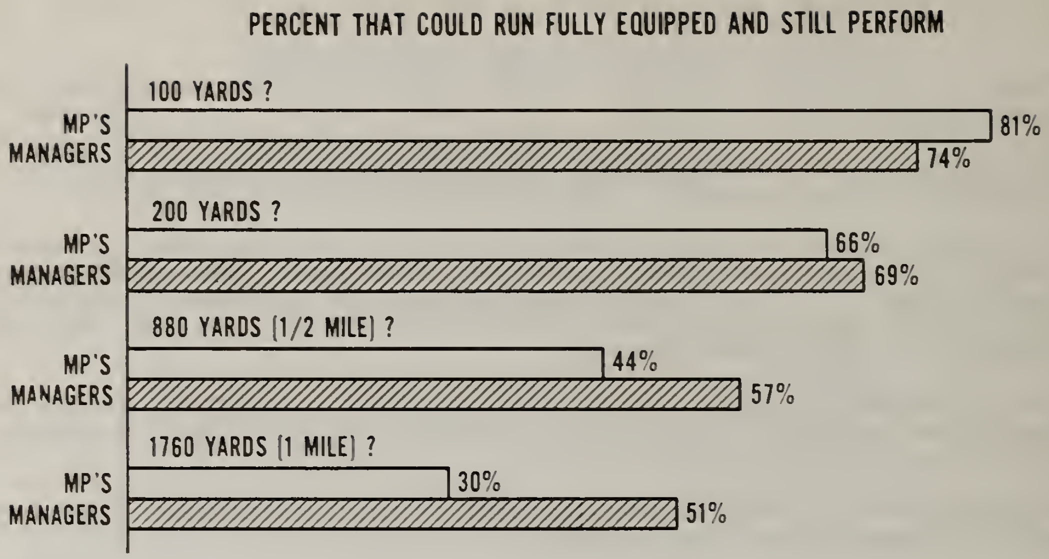

Figure 5. Expected capabilities diverge.

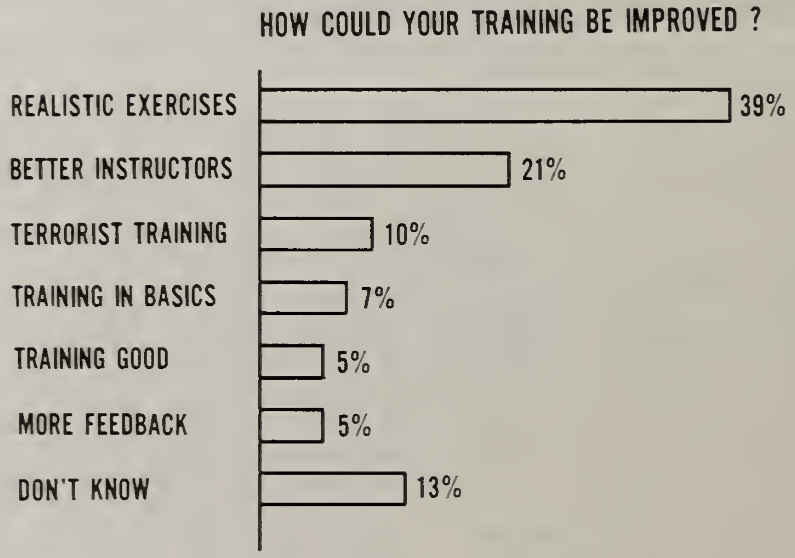

Figure 6. Training needs.

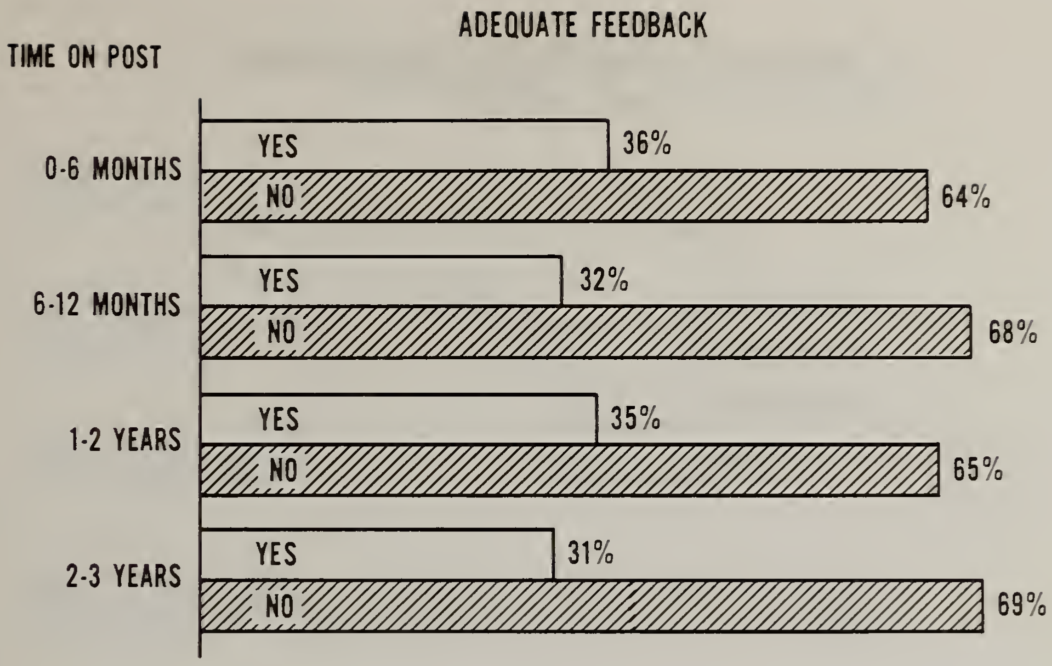

Figure 7. Lack of feedback.

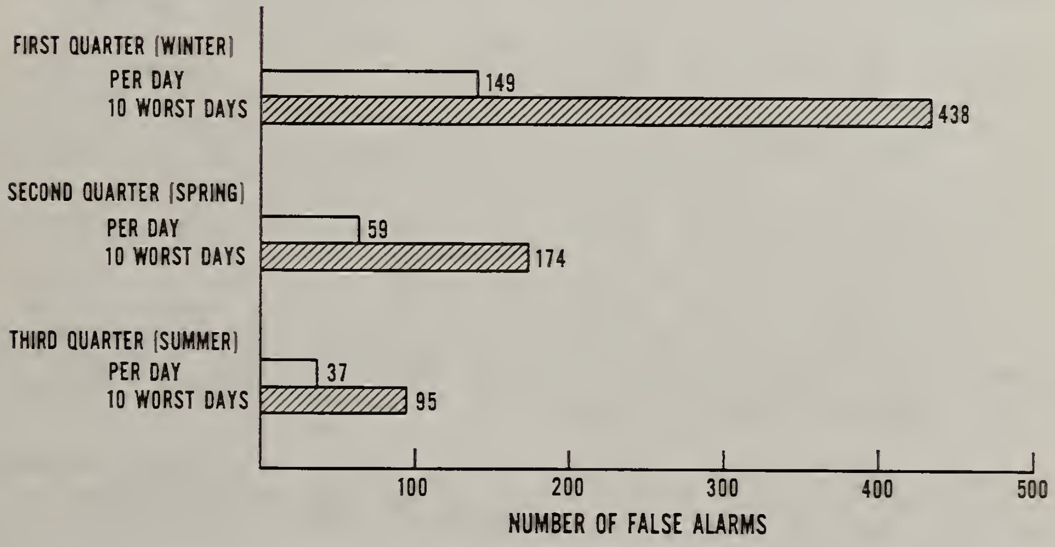

Figure 8. Average number of false alarms per day and for the 10 worst days during the winter, spring, and summer quarters.

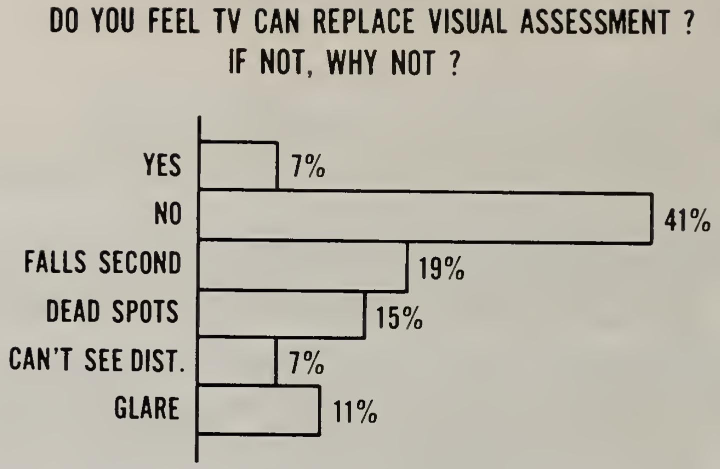

Figure 9. TV is not a substitute for vision.

LTC RICHARDS: You commented on the cameras looking at each other. These were fixed cameras, were they not?

DR. HALL: No, these were mobile cameras.

LTC RICHARDS: So it was a matter of management?

DR. HALL: It is a matter of design error. When you have mobile cameras, with zoom, pan and tilt, and no external targets, you would expect this kind of problem.

Concerning the use of deadly force, the question was asked, "What percentage of the security force would fire their weapon?" under the following conditions: someone standing outside the fence with a gun; someone scaling or coming through the fence; someone crashing through the fence with a vehicle; and, someone inside the perimeter who fails to respond to a challenge (fig. 10). Answers to this type of question should be interpreted with caution because the security guard is faced with a potentially limitless number of complex situations, and the interviewer is seeking answers to a highly abstracted and oversimplified question. Data from related questions indicate, particularly from the managers sample, that there is a good deal of concern over the rules on the use of deadly force. For example, if the rules for the use of deadly force arbitrarily increase the number of judgments and perceptual discriminations that have to be made before the individual can use deadly force, his chances of using deadly force effectively against armed terrorists could be severely impaired.

Another question related to use of deadly force was, "What percentage of the force would be willing to risk their lives at night during an armed attack?" That was reported to be approximately 54%.

"Do you feel it would be possible to have a successful penetration of your facility?" (fig. 11). For sites 1 and 2, 80% of the security force felt that such a penetration would be possible.

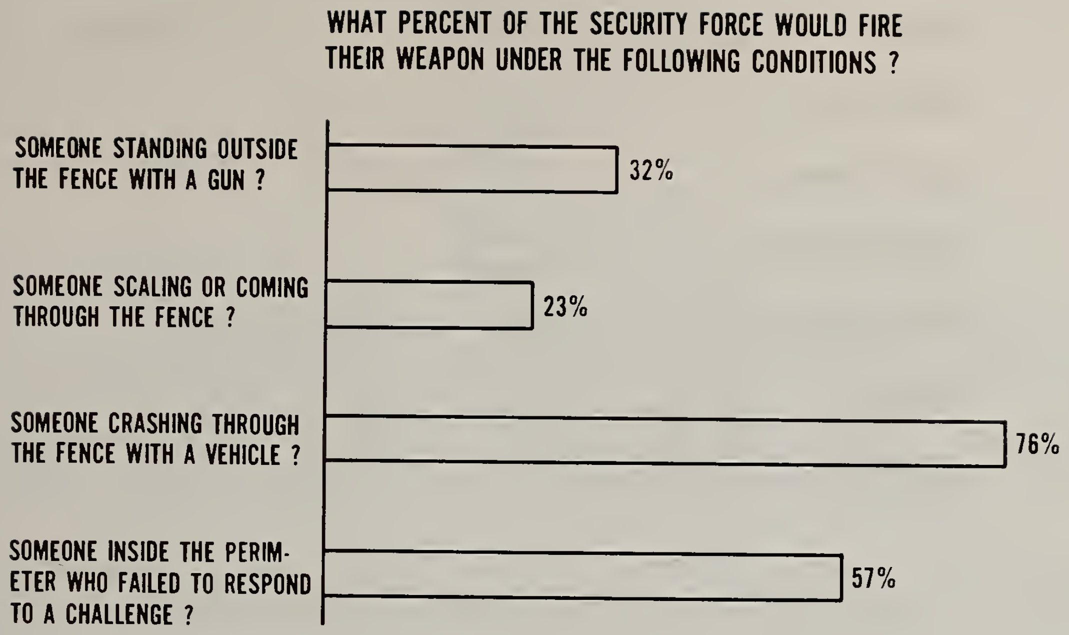

Figure 10. The use of deadly force.

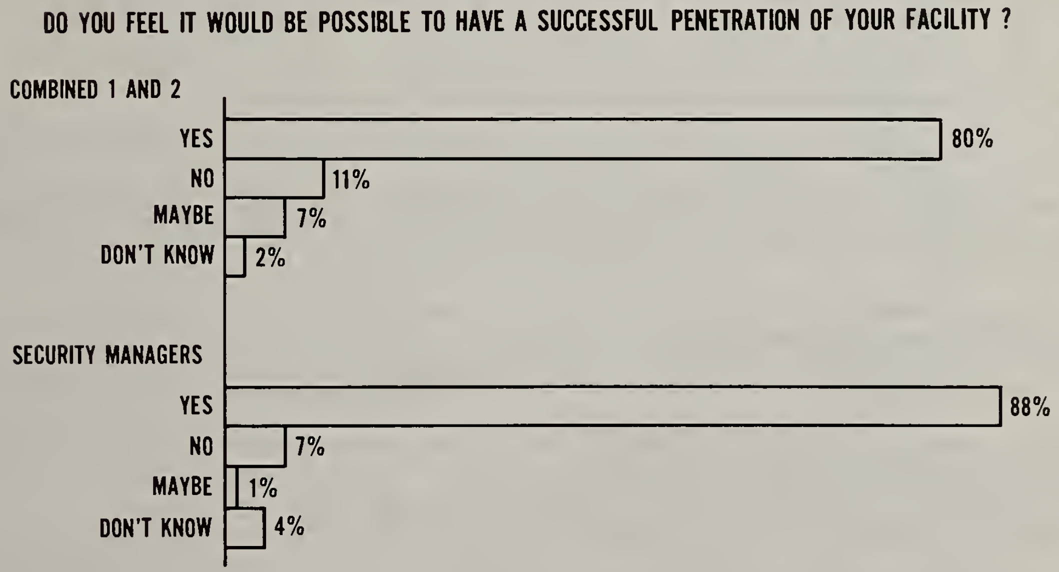

Figure 11. We are vulnerable.

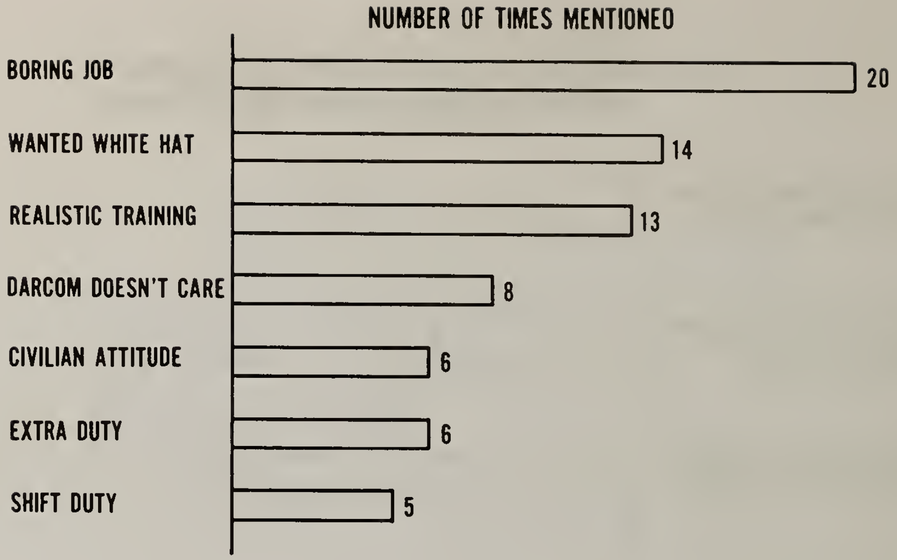

Figure 12. Problems perceived by security manager.

Figure 12 is based on data from the security managers survey and reports answers to the question, "What are seven of the most frequently mentioned major problems that you (as security managers) are confronted with in the process of conducting your job." Once again, boring job, the white hat problem, and realistic training are listed. "DARCOM does not care" may stem from the fact that they feel isolated (complaints about civilian attitudes are mentioned in a number of situations). Some security personnel report that the civilians regard military security personnel as second class citizens. They also report that non-security military people on the normal eight to five work cycle share the civilians' attitude.

LTC RICHARDS: Bob, is that the civilians who work for the government?

DR. HALL: Security personnel report that the civilians employed by the site are not responsive to the military needs, there is a lack of respect for the military.

LTC RICHARDS: Okay, so that is the people in the hierarchy, not the local civilian population?

FROM THE FLOOR: Does that also reflect the civilian security force?

DR. HALL: Yes, it does. Negative views were expressed about the attitudes of the civilian guards.

FROM THE FLOOR: Did you talk to civilians?

DR. HALL: No, we did not, but we do feel it would be very helpful to have a parallel study that looked at the civilian view.

The major topics are summarized below. We can see what might be considered some of the results on the right hand side.

o career objectives	- no future
o PRP	- does not select
o job attitude	- bored
o peer group	- platoon alliance
o physical fitness	- capabilities uncertain
o training	- unrealistic
o feedback	- lacking
o fielded equipment	- abused
	- unloved
	- not a substitute
o deadly force	- confused
o site vulnerability	- almost certain

It is my view that the major problem is the passive job. There is no observable performance product. For example, we do not know the performance envelopes for responding to certain types of alarms and we do not know how reliable security personnel are. Although we have a certain time criterion for personal performance, we do not have data on how well they are likely to perform their tasks in the event of a security emergency. In many instances, we have the wrong equipment, or at least it is used inappropriately; finally, we have the security personnel's own assessment that we are vulnerable.

The recommendations are that we engage in realistic exercises and provide quantifiable performance products at the operational sites. Quantifiable performance products should be measurable, and capable of providing feedback to both the individual performing his duties and to the assessing security manager. The development of quantifiable performance products makes it possible to address the problems of sustained performance, evaluation of new equipment and of new procedures.

We also need competency-based training standards for weapons proficiency at security sites. The development of these standards are dependent on suitable equipment and measurement techniques for collecting the necessary performance data.

LTC RICHARDS: I assume you mean at the site? Surely the Military Police School and the Security Police School have some kind of training standards that they use.

DR. HALL: They certainly do. But because of site peculiarities I think standards also have to be developed within the platoon at the site. That brings us to the development of operational performance standards. We need a reward structure based on feedback from operational performance. By introducing a measurable product into the normal operation, we could present targets and have the individual on duty respond to them. We could measure the time and accuracy of the response to the target.

A good example would be recognition of faces. It should be possible to train people so that they would recognize, by face, every individual that comes through the portal on a regular basis. This is a type of training and performance that can be measured.

Once such skills are developed, they will have utility when the individual leaves security and goes to some related job. By developing a series of observable performance products, we can introduce a set of skills that are important and improve the individual and his potential for his future career.

MAJOR BLAKE: These are Military Police, 95 Bravos, trained at the Military Police School. Did you make a distiction between the training at the Military Police School and on-site training?

DR. HALL: We asked questions about the training at the Military Police School; that is, did they think it was appropriate for the job they were doing. The answers were universally negative; they reported that they only received 6 to 8 hr of training.

MAJOR BLAKE: Okay, but the chart that you put up there before (fig. 6) did not distinguish--it was just "training in general."

DR. HALL: That chart dealt with training at the site--OJT training (on-the-job training).

MAJOR BLAKE: I think that in order to determine whether the questions you are asking are valid, your sample should be larger. I also think it should include GSA guards because they seem to be a more critical factor now than even the Military Police. If these answers were validated by a greater number of questionnaires and you found that only 5% of the personnel want to stay in the security field, how can we base training on a factor of desired performance? We have to, in some way, judge what performance they see as worth their while. If they do not intend to stay in security, it does not make any difference that you perceive (some type of training) as being good for their career.

DR. HALL: If there were a product that was observable, and we could demonstrate skills and improvement, that might change. I do not want to discuss training because that subject is going to be addressed by the next speaker. We only asked some general questions in the area, and that is not our main concern.

FROM THE FLOOR: Could you elaborate on the realistic exercises? Could you define what they should be?

DR. HALL: We have data that indicates some of their comments. They believe, for example, that there should be more SWAT-like training. Many of the present exercises are sort of a superficial rehearsal that really does not give security personnel the opportunity to review and critique (performance) based on real data. It is hard to create realism. I think a very fair question is, "What do you mean by realism?" In simulation realism is a continuum and the actual realism is to bring the bad guys in. Obviously we cannot do that. But I think there could be simulations and competitive exercises that are realistic and valid.

LTC RICHARDS: The problem with a nuclear site is that you still have to maintain security at the same time you are training personnel. That severely delimits the degree of realism that is both possible and safe. At the Agency we are working very hard on developing equipment, such as the laser rifle situation and other things, that can be applied to give a little bit more realism. But you still have the difficult situation of application on your own site while maintaining positive security.

DR. HALL: In summary, my general impression of the troops and managers is that, as the job and tasks are presently constructed, they are doing the best job they can. However, with feedback from simulation and competitive exercises, there is the potential for dramatic improvement in the performance of security personnel.

SECURITY FORCE SELECTION AND TRAINING

Candidate Assessment

Dr. Preston Abbott
Abbott Associates, Inc., Alexandria, VA 22314

Purpose

The purpose of the candidate assessment project was to identify behavioral characteristics best suited for physical security personnel through:

- o assessment of the individual,
- o analysis of the job functions,
- o analysis of job environments, and
- o analysis of training.

From these findings we are seeking ways to reduce attrition of the enlisted and junior officer personnel and to increase job performance and satisfaction.

Individual psychological characteristics of the new security force would be compared (matched) to the job functions (duties) and the environment in which they were performed to determine whether a more effective and satisfied physical security contingent could be developed and/or improved by appropriate training or even positively influenced by systems modifications or organizational change.

Initially it was believed that the job analysis data could be obtained from existing surveys and that the assessments necessary could be conducted at USAMPS, while we reviewed the core training programs. Unfortunately, available job data were inadequate for our purposes and it became apparent that school assignments to specific installations were not sufficiently precise to permit assessing at that location. In the following few months it also was learned that jobs and environments varied too much to generalize from domestic to overseas settings. Our lack of knowledge in these areas was shared by school personnel who were, at that time, dispatching larger numbers of graduates to physical security and to different and unfamiliar locations. Original plans to conduct the research only domestically had to be revised because of these inputs and after visiting one CONUS installation. The project was, therefore, modified to:

- o extend job and environmental analyses to include two major domestic sites and a larger sample of European installations to adequately sample the variability introduced by specific site conditions;

- o include factors of threat perceptions and potential personnel vulnerabilities;

- o plan assessment of individuals after their specific assignments were known;

- o provide training implications data from all sites to identify what instruction could be best presented as core knowledge at USAMPS and those skills applicable to an individual site; and

- o recommend changes in existing or planned physical security systems which might enable a great range of personnel to perform successfully and with greater satisfaction in the job.

Methodology

Interviews were conducted with personnel at all ranks in units dedicated to nuclear security responsibilities. Discussions were held also with other members of the command structure as well as informal groups of personnel who asked to have such discussion sessions.

Only those who volunteered were interviewed. After they answered a series of questions about their job functions and responsibilities--their perceptions of rewards for performance, vulnerabilities in the system, their views of the threat, morale factors, performance indicators, and general reenlistment plans--they could make any additional comments they wished to make. They were assured that their views would not be made known to anyone by name or site. Some biographical data were elicited for research purposes and response grouping.

SOPs and regulations were reviewed at each site. In addition, inquiries were made of the command structure concerning the operations and how they were conducted when the written orders were vague or lacking and incomplete. Observations of individuals performing their jobs were also collected to compare with SOPs and verbal reports.

Progress

Job analyses have been completed at one domestic site except for certain duties, such as convoy protection which could not be observed at the time of the visits.

The job functions observed and the interviews conducted at five foreign and one additional domestic installation have not been analyzed yet.

Two domestic and five foreign sites have been visited and interviews conducted for job environmental data. A report based on the initial data is now in review. Preliminary indicators based on security personnel perceptions were described but cannot be substantiated until the latter interviews are analyzed. It is believed that there will be no startling modification of the more general findings and impressions.

Plans have been initiated to begin the assessment process of both enlisted and officer personnel graduating from programs at USAMPS. The locations for the activity will depend on identifying pinpoint assignments and general flow of the graduates.

The vulnerability data are being analyzed separately and will be used to attempt a profile of characteristics which might be utilized as warning signals for commanders and those engaged in training or assignments. It should also be of some interest to the PRP managers.

Initial Findings*

Tentative results will be reported in two sections. I will discuss briefly some observations drawn from the original sample, principally overseas oriented but substantiated domestically at one site. Dr. Orth will talk about his data on task indicators gathered at one domestic site.

*All of the findings that were verbally presented to the assembly are not represented in this text because of their tentative nature. These results may be made available at some later date if full analysis yields positive confirmation.

We have interviewed approximately 300 enlisted and non-commissioned military police, about 28 junior officers on a one-to-one basis--about 50% in domestic settings and 50% overseas. In addition, we have had informal sessions with small groups of MPs, probably numbering about 50. Discussions have also been held at each site with commanding officers, site security officers--MPs, Ordnance, Field Artillery--and others in the command structure up to depot commanders. (Briefings of initial findings have been given at USAMPS and to representatives of MILPERCEN, USAREUR and TRADOC.) The interviewed sample came from that portion of society where there is not a big alcohol or drug history. They come from what I would call "straight" homes. Ninety-eight percent of the interviewees were high school graduates, with no great criminal record, and are mostly law enforcement oriented. Since they are too young for their local police force this is good training and experience for them.

Dr. Orth will now discuss job analyses results.

METHODOLOGY

Dr. Richard Orth
Orth Associates, Vienna, VA 22180

From the outset, each job analyzed was required to be available for applying three methods of data collection.

- o Direct observation and/or experience
- o Review of written material
  - Training manuals
  - Job guides/regulations
  - Records
- o Interviews
  - Job incumbents
  - Supervisors
  - Management

Since the Military Personnel Center (MILPERCEN) uses the questionnaire approach, this effort was not duplicated. The present research, however, points out some of the limitations of this approach. The most striking limitation is that one must be conversant with the entire range of the job before the questionnaire approach can be used to its full potential.

Although the jobs could not actually be experienced, each job was subjected to repeated observation as it was being performed by different incumbents and under different situations. This procedure yielded a great deal of data about behaviors that had become part of the MP's habit structure and generally not recalled during questioning.

Reviews of the written material provided the background for the job. They also provided knowledge about thc theoretical requirements of the job, the assumptions that are made about performance requirements, and the legal requirements. The major source of data turned out to be the local guard orders which govern the troops' behaviors on the job. However, the governing regulations such as AR 50-5, USAREUR 50-100, ED 60-10, and FM 19-30 provided additional information about degree of liberty that is, and can be taken with the regulations. The broad job analysis techniques include:

- o Questionnaires or checklists from:
  - incumbents
  - supervisors
  - management
- o Psychological or physiological tests
- o Direct observation or experience
- o Review written works:
  - Training manuals
  - Job guides/regulations
  - Records
- o Interviews with:
  - Incumbents
  - Supervisors
  - Management

The interviews with both the incumbents and their supervisors provided a broad range of information about the jobs. In summary, the interviews yielded information about each respondent's perceptions about the job, in addition to the salient tasks that are performed in completing the job.

The supervisor and management interviews were reasonably simple and straightforward. Most of their perceptions about the job seem to be based upon the written requirements against which they perform their inspections of the troops as they are performing their jobs.

The interviews with the job incumbents took a turn which relied heavily upon the observations that had been performed prior to the interviews. The troops took such a generalistic approach to the job that they rarely considered any specific behaviors. In many cases, the interviewee was confused by being asked to describe his job. In these instances, they were prompted by illustrating the first two or three behaviors that were performed at the beginning of the shift.

PERIMETER PATROL

Perimeter patrol is one of the jobs that virtually every new MP performs at the domestic sites visited. It is necessary for the purpose of presentation to combine behaviors into task groupings. This method ignores some of the idiosyncratic responses and gives a better feel for the job than the specific behaviors.

The major components of the job are quite clear.

- Supplement electronic sensing equipment
- Prevent intrusion
- Keep damage minimal should intrusion occur

Just as clear are the official task groupings.

- Keep patrol log
- Check route on guard orders
- Check vehicle
- Check radio
- Drive vehicle on prescribed route
- Visually check barriers
  - From truck
- Visually check culverts
  - From truck
  - From ground
- Visually check gates
- Note and challenge other vehicles
- Respond to challenge
- Report patrol status regularly
- Report status of area regularly

These job components and task groupings can generally be gleaned from the guard orders or from the Soldier's Manual for the 95B MOS. Some, however, are found to be specific to a particular platoon and are part of an unwritten set of SOPs. It must also be cautioned that these tasks can be ignored by the job incumbent. These are areas where the troops have set up a system among themselves that allows a foreshortening of this official task structure by avoiding repetition.

The unofficial tasks are often considered to be the important ones. When standing guard at an inactive sensor, the patrol must focus on that one spot. He may have no distractions, he may not smoke, eat, or drink while doing his task. He simply sits in his truck and watches the spot in the barrier.

Unofficial tasks are:

- o Guard an inactive sensor site
- o Visually check area inside and beyond barriers
- o Respond to messages sent in 10 series with 10 series
- o Pass inspections from the following while performing job:
  - Military police duty officer
  - Sergeant of the guard
  - Patrol supervisor
- o Provide newcomers with on job training

The task of checking areas inside and outside the barriers forces the guard to make decisions. There are no clearly marked sections which define his area of responsibility. He simply uses his own judgment or his range of vision to determine the area of responsibility.

The so-called 10 series are used for radio communication. Even though the guard orders may read that they should not be used in emergency situations, they are still used and, in fact, are used even more. (Many troops take subtle pride in their ability to use the series, but they befuddle--sometimes intentionally-- the uninitiated.) Moreover, the troops at the domestic sites use the Highway Patrol version of the 10 series rather than the one taught at the MP School and used by the white hat MPs. In addition, they have added some elements to the series to describe particular situations which have strictly local meaning.

Standing inspection is considered a normal part of the shift for the patrol and the troops are generally prepared. The conduct of the inspections, however, is a critical part of the job environment. Because of platoon differences in some SOPs, the troops must know who the duty officer is so they can be prepared for the way he conducts the inspections. They generally know how their own SOG will conduct these inspections after they have been on the site for a short time. The other platoon leaders and platoon sergeants, however, may continue to surprise them.

The major focus of the job analyses is to try to arrive at some conclusions about how assessment and candidate training can improve not only retention, but also job performance. Some of the initial hypotheses were:

- o Assumption that they have basic aptitudes or skills such as:
  - Driving
  - Vehicle inspection
  - Radio usage
  - Weapons
- o Inadequate definition of job
- o Repetition in tasks
- o Non-happenings = success
- o Sense of isolation
- o Maintenance of readiness

Although it may seem that these assessment factors dwell on negative factors, this is the reality of the situation. If all were positive, there would be no need to go through the exercise, because everyone should be content with the status quo.

First, some tacit assumptions about basic aptitudes or skills possessed by the guard who performs the patrol function are made. It is probably safe to assume that the average guard can drive. (If he can drive a truck safely is another question.) The aptitude required for first-level vehicle maintenance or even detection of problems is clearly not possessed by everyone. Usage of the radio, especially the 10 series, requires some skills that not all possess. Weapons usage is a problem when one considers the fact that some, such as the M-60, may be too heavy or too difficult to maintain for the smaller or weaker troops, and, more importantly, their exposure to them is very limited.

As was illustrated by the list of official and unofficial tasks, there is often no clear definition of what is expected of the guard in this job. Many of the duties are not stated, and he must be willing to define the job himself. In other cases he must respond to changing requirements imposed by the supervisory personnel.

Some of these implications are obvious. For example, the tasks are extremely repetitive. The patrol does the same thing every 20 to 30 min. The only deviation is when there is a test and even these become repetitive after a while.

The foremost characteristic of these jobs is that they are best performed when nothing happens. The rewards for such are not what we are used to. The soldier must be found who can take pride in the fact that nothing happened and who does not need to tell anyone about the state of affairs that is his source of pride.

The patrol guard suffers from a sense of isolation when he is on duty. This is true of some other jobs as well. The interrelationships of all the jobs within the security force are not clearly stated so the patrol guard does not really feel part of the team. The sense of isolation is enhanced by the fact that the guard does not always know his relationship to the other people who work on the site. On top of all this, the sites are in relatively remote locations which gives the guard a feeling of isolation from society.

Finally, a major assessment factor is the necessity for the patrol guard to remain vigilant even though all the forces around him compel him to withdraw. The repetition, the boredom, the loneliness all contribute to his going to sleep, figuratively, or actually, when his primary task is to be awake and aware of everything that is going on.

RESPONSE FORCE MEMBER

The response force is one of the commonly held jobs at the European sites. Some of the official tasks are more appropriate for the past because there has been a change due to the reaction to AR 50-5. The changes are reflected in both USAREUR 50-100 and ED 60-10, but are not yet in all the guard orders. The response forces no longer have the response times that were associated with the SAT and BAF concepts. Rather, the response time is now geared toward having the entire force in position within 5 min. Thus, the times are omitted unless needed for illustration of a point.

Task analysis for this group is extremely difficult. There are several different jobs within the response force that may deserve separate analysis. For example, the M-60 gunner has a unique responsibility within the force as has the M-203 gunner. They have specific functions within the secondary response force team. There are, however, enough commonalities among the sites in their description of team concepts to allow a general set of tasks to be derived. Moreover, the jobs are shared with little permanence to any one job, so that the respondents describe themselves as SAT or BAF team members rather than M-60 men or M-203 men. Thus, the present report will discuss the combined response force rather than the individual jobs. The list of official tasks that were common to all sites were:

- o Respond to site of alarm as a team
- o Take up a good firing position
- o Assess the situation
- o Keep in communication with supervisor
- o Have magazine in weapon (no round chambered)
- o Establish a field-of-fire capability

- o Prevent theft, damage or other harm to items
- o Maintain a state of readiness when not at an alarm
- o Make regular checks that may be part of the informal SOPs
- o Wear proper uniform for responding to alarms
  - web gear
  - weapons
  - bolt cutters

Some, such as the means of responding to an alarm, are omitted because of differences among the sites. Some require response on foot, some by vehicle. The differences were only partially attributable to the size of the site.

Before the unofficial task list is presented, the reaction to the changes in nomenclature should be discussed. It affects both the job analysis and the guard's responses to the interviews. There seems to be an almost universal tendency to retain the separate SAT and BAF concepts. The closest to any change was labeling the SAT an assessment team. In concert with this distinction, the unofficial task list is divided into two sections. The unofficial task list for the SAT includes:

- o Respond first and assess situation
- o Deploy either on scene or as leaving SSCC
- o Use good infantry tactics and ignore SOP
- o Be prepared to shoot intruder
- o Put life on the line
- o Use radio, vehicle, bolt cutters, etc. as needed
- o Know and use halting procedure with duress code and password
- o Conduct sweep of the area
- o Determine necessary amount of force

There are several notable points in the list given by the MPs. The first is the necessity of infantry skills. They must know how to deploy, how to use fire-and-maneuver, how to keep in communication with the rest of the team. The second point centers upon reaction to intruders. They feel that they would probably shoot anyone there if they had a chance. Most felt that they would be killed by the intruders, and communicate the situation by their own death rather than by telling the BAF what is going on. There is a general feeling that if the alarm is real, this is a suicide squad. Because of this, most would only maintain the SOP to cover themselves in case of command censure.

Several other tasks appear which have grounding in the guard orders, but leave the method up to the guard or the platoon. The SAT conducts the sweep of the area after the BAF arrives. The SAT (and BAF) has a set of bolt cutters to allow access to the limited area. No one who was interviewed had ever tried to use the bolt cutters to gain access to the limited area.

The task list for the BAF portion of the response force is much more limited:

- o Support the SAT
- o Deploy in predetermined areas, deploy as needed
- o Set up a field-of-fire and cover the front of the structures
- o Set up the M-60, the M-203, and the M72A2 LAW
- o Contain intruders for the augmentation force
- o Determine necessary amount of force

The major function of the BAF is to act in concert with the SAT to prevent any damage from occurring. Once again, knowledge of infantry tactics is vital. The concepts of field-of-fire and deployment will be employed by the troops when they respond to an alarm, but they will most likely <u>not</u> respond to the predetermined areas. This is because they feel the intruders will be aware of the SOPs and would simply wipe out the BAF. The M-60, the M-203, and the LAWs are seen by some as very helpful to the mission and by others as worthless. The latter group is pessimistic, because they feel that these weapons will not come into play because the gunners will be killed as they deploy or get the equipment (LAWs). This team, much like the SAT, feels like a stop gap to hold the intruders until the augmentation force arrives.

The implications for assessment are much the same as those discussed for the perimeter patrol. The primary distinctions are two: these teams have to be able to go from a state of relaxation or sleep to total alertness within 1 min, and they feel very much like suicide teams whose job it is to sacrifice themselves so that the "real response force" has time to arrive. There must be a real willingness among these individuals to discard the MP and adapt the infantry methods of dealing with problems.

CONCLUSION

Some of the results presented are preliminary. The changes resulting from the "15 in 5" concept had not been completely integrated into the habit structure of the security forces.

There are a multitude of environmental factors which future analyses will reveal more clearly. Questions of leadership in an environment where unit (company) identity is lost seem pre-eminent among the job environment factors. Indeed, there seems to be a loss of identity with the MP Corps and many of the troops feel they are more infantry than MP.

The entire process, from enlistment, through training, to job definition, seems to force the troops into a position of feeling lost. Little or no mention is made of physical security until the soldier feels it is too late to do anything about it. That physical security is an ill regarded position is enhanced by that fact, by the teasing that the troops suffer from many of the instructors during the latter stages of AIT, and by the fact that the reward for performing the job well is a ticket out of physical security.

Such results, plus many of the basic aspects of the guard orders, indicate that there are issues which transcend the specific site. The obvious need for training in basic soldiering skills, the need to clarify some organizational issues, and the need to attend to the human factors associated with the jobs are just a few of the issues which will be addressed in the future analyses leading to the development of useful assessment methods for physical security forces.

STANDARD ERGONOMICS REFERENCE DATA SYSTEMS (SERDS)

Dr. Harold P. Van Cott and Joel Kramer
National Bureau of Standards, Washington, DC 20234

In his Presidential Address to the American Society of Mechanical Engineers in 1914 James Hartness said:

> "The engineer's knowledge of mechanisms has always made it possible for him to design machinery, but since machinery must fit man it must be developed with a full recognition of man's characteristics."

As technology has grown more complex, the truth of Hartness' statement has been repeatedly confirmed. It is now generally recognized that if the benefits of technology are to outweigh its penalties, technology must be designed and evaluated using reliable, accurate data on the characteristics of the individuals with whom that technology will interface.

In this century great strides have been made in perfecting measurement methods for obtaining reliable data on the physical and chemical properties of substances and materials used in technology. Important advances have also been made in the critical evaluation of physical and chemical data. However, progress along these lines in the field of ergonomics has been much slower.

"Ergonomics" is the science of the measurement of human characteristics and the application of these data to technology design and standards. Ergonomics provides an empirical basis for making objective engineering judgments about the interface between man and machinery.

Ergonomics data are obtained from measurements of known phenomena made under controlled laboratory or field conditions. These measurements are obtained from samples of individuals representative of the population that use a product, equipment or system.

Ergonomics data fall into three major classes:

- o Measures of behavior, or response
- o Measures of physical anthropometry or body size and body dynamics
- o Measures of physiological response.

An example of behavioral data is the range of physical energies to which the human senses are responsive. The sensitivity of the visual system, for instance, ranges from 400 to 700 mμ for all but color deficient individuals. Energies outside that range evoke no visual response and cannot be used to transmit information to man.

An example of anthropometric data is the distribution over a population of peak forces, in Newtons, that can be exerted in turning a lever or handle.

Physiological response data include human reaction to chemicals, electric shock and mechanical blows.

If examples of ergonomics data such as these are available, why is there a problem? Why do we need to consider going further and doing more than is already being done as a normal part of our individual applied research activities? As I see it, there are several serious problems in measuring, evaluating, and making ergonomics data accessible. First, we do not have standard ergonomics measurement methods or technology. Researchers tend to develop their own approach to measurement, use their own equipment for capturing and recording data, and have their own way of reporting it. As a result, some ergonomics data are inconsistent, and some are inaccurate. The different measurement methods that have been used have often been applied to highly specialized populations, such as the military, and cannot be extrapolated to other groups. In the United States, for example, the most recent survey of the anthropometry of the entire U.S. population was made in 1941, and has since become obsolete due to diet and exercise factors. Other ergonomics data have also become obsolete, much of it dating back to World War II. There are gaps in ergonomics data; there are some areas in which we simply have no good normative, accurate, and up-to-date information. Finally, except for the process of peer review that occurs prior to journal publication, there is no systematic critical evaluation of ergonomics data. There is no individual or group that has as its primary goal the systematic evaluation, screening and integration of ergonomics data. In my opinion, these are serious problems which greatly limit our ability in using an applied science to help solve the problems of which we are potentially capable of solving.

In 1977 at the National Bureau of Standards we began a project to examine the need for standard ergonomics reference data. I reported on that project at your second annual symposium so I will only summarize it here.

During that project we met with groups from NBS, other agencies, industry, trade associations and the research community. We examined the status of the existing ergonomics literature and assessed the measurement technologies that could be used to collect new data. From that project, reported in NBSIR 77-1403, which I will be pleased to mail to anyone who requests it, three conclusions can be made:

- o First, there is a widespread demand for reliable ergonomics data by industry, the research community, and governments.

- o Second, that demand cannot be met by existing ergonomics published data alone.

- o Third, a technology for ergonomics measurement is needed to supplement the information not adequately covered in the existing literature.

In light of these conclusions, we developed a concept for producing reliable standard ergonomics reference data.

The concept is simple. Critical evaluation of existing published ergonomics data will be performed by the National Bureau of Standards, universities and other organizations with specialized scientific competence in selected areas of ergonomics. Data from this process will constitute one input to a collection of ergonomics reference data.

Since existing data in many instances are obsolete or inaccurate, they must be supplemented by new data in key areas. To obtain these data will require the development of standard measurement methods and technology and their use to collect new data or validate existing data. The new data would be added to critically evaluated data from the published literature to provide a comprehensive base of reliable ergonomics information.

Users would help establish priorities for the data to be critically evaluated and collected. Priority choices would be based on:

- o The existence of a widespread need for data of a given type,

- o The ability to characterize the phenomena to be measured, and

- o The ability to develop and apply measurement methods and technology that provide reliable data at a reasonable cost.

Phenomena that are poorly understood or that cannot be objectively measured would be excluded.

In 1964, the U.S. Congress authorized the formation of a National Standard Reference Data System. This system consists of evaluated data on the physical and chemical properties of materials and substances of widespread use by industry and the research community. Critical evaluation centers collect and evaluate the existing published data, integrate it, eliminate data that is of questionable quality, and provide the screened and evaluated data by means of critical data tables and computer tapes. This system, which is currently managed by the National Bureau of Standards, provides to all users the best, most accurate data on such physical properties as the melting points of metals, the properties of polymeric substances, and other data. As a result of the successful operation of this system, being coordinated with industries and universities throughout the United States, we now have far more accurate, reliable and precise data concerning such things as the melting point of tungsten than we do about visual acuity, human reaction time or the anthropometric dimensions of the human body.

In our opinion, a standard ergonomics measurement technology can be developed using state-of-the-art instrumentation to obtain measurements of human characteristics. However, this instrumentation must be integrated into compact, cost-effective units, calibrated and tested in the laboratory, and tried out in the field to insure a valid approach to measurement.

Let me illustrate the challenge of developing this technology with some examples.

Manual anthropometers, consisting of simple tapes, rules and calipers have been widely used for the measurement of human body dimensions--lengths, circumferences, surface areas and body proportions. These devices, even in the hands of the most skilled person, are time-consuming to use and subject to measurement error.

The need for increased speed, accuracy and reliability of measurement has been met in part by the partial automation of these anthropometers. However, neither technique provides a permanent record from which new measures can be obtained once the person measured is no longer available. For additional needed measurements, either the same individuals must be remeasured or a new sample obtained at additional expense.

New imaging techniques will help solve this problem. These techniques include single and multiple camera photography, biostereometrics, holography, and ultrasonics. Each technique must undergo comprehensive technical evaluation, comparison and cost-benefit analysis before the most suitable mix can be identified.

One promising technique uses three cameras to take front, side and back views of an individual. The person being photographed is illuminated by a pattern of dots. The photographic images are then electrically scanned and the X-Y coordinates of selected dot pairs which represent body reference points are used to generate a computer diagram of the individual.

These are only a few of the approaches that can be taken to improve the speed and accuracy of measurement.

Now I will turn the meeting over to Joel Kramer who will describe our survey of user needs for ergonomics data.

MR. KRAMER: Subsequent to the development of the concept of the system, we found the need to conduct a user need survey. We have distributed about 4400 questionnaires, to trade associations, professional societies, and standards organizations, to assess the current usage of ergonomics data, to identify the sources of data to determine the degree of satisfaction or dissatisfaction with such data, and to gage the impact of a standardized ergonomics data base.

We hope by the end of August or middle of September to have the results. The Defense Nuclear Agency was asked in the latter part of FY-78 by the Director of Research and Engineering to investigate the need and feasibility for establishing a DOD Physical Security Data Base and Analysis Center. The Law Enforcement Standards Laboratory (LESL) at the Bureau of Standards was asked to explore the feasibility of incorporating DNA ergonomic data requirements within the scope of the proposed NBS research program. A small-scale effort was launched at the end of the last fiscal year to conduct a preliminary evaluation of DNA physical security ergonomic data requirements with emphasis on existing ergonomic data banks.

There are numerous potential applications for ergonomic data to improve functional performance of security systems and enhance the performance of the guard force. Work/rest cycles, guard adaptation, reinforcement techniques for personnel while in training and on duty are a few examples of the factors that should be considered when developing operating procedures. Human sensory capabilities are of the utmost importance in examining the interface between the operators and equipment. When operating in an unstressed and unthreatened environment, people can adapt to poorly designed equipment or inadequate procedures. However, the individual's ability to use poorly designed equipment or inadequate procedures can deteriorate rapidly in an emergency or highly stressful situation, greatly increasing the likelihood of mistakes and accidents. The data domains within the field of ergonomics range from body dimensions to basic sensory processes, reaction time to higher order processes, decision-making, performance, and learning. I think you can see some concrete examples of how such data might be related to physical security problems guard forces encounter.

In addition to investigating DNA ergonomic data requirements, we have proposed for this coming year the continued development of a thesaurus of terminologies and definitions, breaking the areas of ergonomics into more specific data subdomains.

STATUS REPORT ON THE NBS VIGILANCE RESEARCH PROJECT

Dr. John V. Fechter
National Bureau of Standards, Washington, DC 20234

My presentation will cover the details of a multi-year research project on the vigilance of guards at nuclear weapons storage facilities. Because we have not completed contract negotiations with the firm that will be performing a review of the published vigilance literature, a first part of that project, I will also try to cover that material in my presentation.

Let me start by describing the origin of the vigilance project and also some major changes we proposed for it after we began in fiscal year 1978.

Originally, NBS was asked to perform a detailed review of published vigilance research. Using the results reported by others, we intended to identify the relationship between individual differences, operating procedures, the man-machine interface, and environmental conditions that enhance or degrade human vigilance. This sounded like a basic research proposal, to find out what has been done and then apply it to the physical security application.

On the basis of that review, sets of formal research hypotheses about things that might be done to improve vigilance at operational nuclear weapons storage facilities would be proposed and experiments begun to actually verify those hypotheses.

When beginning this project, we went through some very deliberate considerations to define exactly what we were trying to measure--what was vigilance? It means one thing to the human engineering field and it means something entirely different, in many cases, to a base commander or a person walking the perimeter fence. We could not effectively review vigilance literature or generate any reasonable hypotheses unless we had a firm definition of the tasks the nuclear guard forces are expected to do, which of those tasks are in fact related to nuclear security, and what kinds of vigilance are required of the guard.

Defining the criterion of effective guard force performance was difficult, especially in light of the surprising results reported by Abbott Associates and Mission Research Corporation. When redefining effective guard force performance in light of those findings, we concluded that the original approach we had started would be incomplete and likely to produce results of doubtful application to real-world situations.

I am confessing by saying that we started off on what we now consider was the wrong foot. We would have produced some results of dubious application in light of the real-world problems and requirements of the guard forces that we found to be outside the original definition of vigilance we had been assuming and working with.

Our revised approach considers the guards as micro-systems or micro-security systems unto themselves, who may or may not be elements in a larger security system. This may be the case on the basis of procedures at the base or it may be the case based on the perceptions of the guards. They may feel they are acting independently or the platoon is acting independently and may not see themselves as an element within a larger physical security system.

We are also considering only the vigilance aspect of the many problems and issues related to effective nuclear guard force performance. We are not trying to tackle all the issues of training, feedback, or operational procedures. But we think that vigilance is a main component and we can concentrate our efforts on it.

We are now prepared to consider the significant parameters of work shifts, specific sites, and total system factors in our research. We have "seen the light" from the results of Drs. Abbott and Hall and we have revised our plans accordingly.

What I would like to discuss now, reflects our revised approach and what we consider a logical plan of empirical research to produce specific procedures for use in field settings--procedures whose long-term effectiveness can be evaluated, and then actually implemented by base commanders on the basis of those evaluations.

Humans, as we consider them, are an active ingredient in each and every aspect of the physical security system, and are in reality a security microsystem to themselves. If they have to, they are capable of accomplishing all the security functions independently and unaided by sophisticated mechanical, electromechanical, electronic, or optical aids. This can be the case; it usually is not in most physical security installations. Human behavior, then, is of the utmost importance to those who are trying to design, staff, or implement operational physical security systems. The aspect of human behavior that we consider essential to the performance of the individual assigned to any security function is vigilance, and we are focusing on that element.

Throughout its existence, DOD has been faced with the problem of selecting personnel for specific assignments. Problems in selection and training have already been mentioned. In recent years, the problem has been further aggravated by the concept of the all-volunteer force and a commonly accepted reduction in the educational level of new recruits. Traditionally, DOD personnel assigned to guard force security functions have been selected by default (this conclusion is based on comments during workshops at the third symposium). That is, they represent personnel who are not qualified or interested in high priority assignments in the normal recruiting and selecting process.

As a result, the guard may be characterized as a high school dropout of limited capability. (Now, again, this reflects comments during the third annual symposium and does not reflect the comments of what you learned from Dr. Abbott.) But in general, these people do not have the qualifications or the experience to work with sophisticated, large-scale physical security systems. This may be the fault of the individuals involved, the fault of the training, or the procedures actually used at the base installation. At the same time, I should also emphasize that the individuals apparently (from the interview schedules) do consider their jobs as very important, as something that has to be done, and they do have the element of patriotism and interest in their job. As was said earlier, they are trying to do the best they can under the circumstances they are placed in.

DNA, through its active participation in the last three behavioral science symposia, has stimulated the interest of many behavioral scientists to specialize in areas that apply to nuclear security guard forces. Practitioners have frequently focused--and this was a major emphasis in the last symposium--on studies of motivation, selection, training, and job enrichment as investigations that hold great potential for finding principles that can be immediately applied to enhance the guard forces. Investigations in these areas for the most part would be directed toward procedures and personnel policy that are or should be under the control of people responsible for administering the physical security function within DOD.

But research investigations of human behavior are never simple or straightforward. Human behavior is complex and subject to the influence and effect of many factors, many of which are so subtle it is impossible to measure in the short run. It is frequently impossible to isolate a single factor that impacts human behavior. Even those topics that have been discussed earlier will overlap to some extent and all are influenced to some degree by common human factors such as demographic characteristics, socio-economic environment and experience, and individual mental abilities and past training and experience.

The key to behavioral research of security forces is to identify a valid means for measuring human action that can serve as a criterion for assessing existing performance or assessing changes brought about through modified behavior, or circumstances. We are trying to find appropriate parameters to measure performance. You need a criterion against which the guard force can be rated by themselves and against which their performance can be rated by the management structure.

Factors that impact performance but are not measures of performance directly, are such examples as tardiness; excessive use of sick leave; very lengthy, extended lunch hours; and general job dissatisfaction. These, again, are projected indicators of performance but are not the performance you are trying to measure. Similarly, enthusiasm, professionalism, and dedication are also considered factors related to effective guard force performance, but are tangible factors that are very difficult to measure. You can say someone is "professional," but you have the same problem we had in defining what is vigilance: what is professionalism? It depends on who is doing the rating.

We are not trying to duplicate any of the work that was done beforehand, but instead want to capitalize on that work and go from there, applying it to the area of vigilance.

While DOD has not necessarily attempted to define measures of guard force performance in a manner that relates human behavior to operational requirements, some of the criteria used to rate a response force unit during a facility inspection or in making observations of that unit when on alert, are typical of the parameters that would be investigated by the behavioral scientist. Those wishing to significantly enhance the performance and capabilities of the response force must expand on the customary military observations and also identify second and third order interactions that can be used to pinpoint factors lending themselves to change in behavior in a positive direction. You cannot simply describe the guard force's performance related to passing inspection or problems raised during inspection; we also have other long-term morale problems and other social factors and environmental factors that can be measured and should be measured because they are directly related to effective guard force performance. The entire system has to be considered.

I described our approach as considering the guard as a system, but to consider the guard only as a microsystem unto himself without considering how he interacts with the rest of the system, would be a mistake. To study one parameter of guard force performance without considering the other factors--political, social, experiential--would also be a mistake.

The role of a security guard assigned to a nuclear weapons storage facility is generally accepted to represent the worst of all possible duties. An individual may be subjected to extremes in climate, isolation, and most certainly boredom. Because the individual normally has little to look forward to in terms of promotion or better duties, the assignment is often considered a no-win situation. The guards do as much as they can to avoid making a mistake in the absence of any opportunity to demonstrate competence. There is very little opportunity for a guard to show that he is effective. If you do not have an attack, if you do not have an event to detect, you cannot reflect your performance to your superiors; you cannot show how well you are doing your job.

The guard is under pressure to perform at an acceptable level, but probably finds it difficult to believe that there is any real reward for so doing. And worst of all, the guard is required to maintain constant vigilance to protect against an event that in all likelihood will never occur, based on the past experience.

The purpose of the revised NBS vigilance project is to assess those factors that influence the individual state of vigilance and to develop methods to improve this aspect of performance on a daily and long-term basis. For the purposes of this study, vigilance is considered as a complex set of human behavioral factors including detection, recognition, and identification of stimuli, and the appropriate response to those stimuli; also including intelligence, which is the analysis of stimuli, the environment, and other information sources recognize individual threats to security, patterns of events, or unusual combinations of incidents that warrant investigation because they may constitute a threat to security. People should be attentive not only to the TV display and not only to things they see as an immediate threat--a person or a vehicle coming through the fence--but also to unusual patterns of sensory responses, unusual patterns of local behavior.

The extent to which the individual is capable of behaving in a vigilant manner is influenced by job-related factors such as specific training and learning from peers, supervisors and others; by the weighting scheme applied to the cycle of detection, recognition, identification; and, most importantly, by the response. Many guard forces learn what responses are appropriate to make and what responses are inappropriate to make as a function of their perception of the local command or the local boss instead of the actual, standard operating procedures.

Also, the extent to which a person can behave in a vigilant manner is influenced by stress induced by job pressure; circumstances such as imminent threats, or fatigue; associated duties not strictly related to the protection of assets per se such as answering the telephone or entering data in log books and other kinds of paperwork. It is also influenced by the characteristics of the workplace.

In addition to job-related factors, the ability of the individual to maintain a vigilant state is influenced by a variety of personal parameters--physiological factors such as health and appropriate rest while off duty; emotional perturbations such as marital problems, anxiety over financial affairs, and drug or alcohol abuse; social problems such as community and group acceptance; quality of life in general; and privacy or the lack thereof. This may be a most important finding from the Abbott and Hall work--a lot of people assigned to guard force duty do not feel they have any control over their personal privacy because they are always subject to call, even after the regular work cycle has finished. This is true whether the call is for training or for relieving someone else who is not on duty, or insufficient staff in the first place.

By considering individuals as micro-security systems unto themselves, operating in a larger system, it should be possible to independently assess the parameters that influence vigilance on all levels--basic detection behavior, job-related, and personal.

The program will deal initially with individual vigilance behavior. This will involve two basic tasks: the first is to analyze the laboratory data obtained during experiments conducted to study vigilance as a generic topic. We want to develop the best case for vigilance, that is, the best case in the absence of stress, the best case in the absence of real-world factors, such as answering the telephone and walking the beat. We want to find out how fatigue, work-rest cycles, and parameters in that category are influencing vigilance ability--ability to detect an unknown signal, ability to recognize strange patterns of events. That would be best case, and you could assume then that the real-world situation would always be less than best case. At the conclusion of that phase we would know where we were before we started any field experimentation or any laboratory experimentation started on a specific vigilance factor. This phase should also point out any serious gaps, inconsistencies or discrepancies between studies. It is important to have that critical evaluation done to make sure you are not basing your study on some conclusion which has been invalidated by other research.

We also intend to do a detailed analysis of the findings of the Abbott and Hall studies of guard force selection, training, and duty.

I am going to briefly describe the project plan, a three-phase program to be performed over a period of 3 to 4 years. The first phase is Human Factors Assessment and Field Observation--Selecting Guards and Performance Criterion. Primarily, this is analyzing the results of the previous Abbott and Hall study to determine what is truly expected of nuclear weapons guards in operational settings. We are not basing this on training, we are trying to find out what the real-world expectancies are. Second we will analyze the Prior Vigilance Research data. Third is the Behavioral Science Symposium that is in progress right now.

We would then like to do field observation studies after identifying specific vigilance tasks that we can measure. We want to consider as many areas as is reasonable in the area of isolation from or proximity to population centers, cold-hot and humid-dry environmental considerations, levels of instrumentation and electronic augmentation of senses at facilities (instrumentation impacts greatly on the kind of vigilance a person is required to have).

It is our opinion that we will be in a position at that point, to commission some laboratory studies of specific scenarios to be investigated. The vigilance scenarios will be studied so that we can determine whether vigilance would or would not be improved given certain parameters or circumstances. Field validation would follow those laboratory scenario tests that were successful.

When the laboratory scenario results are available, we will propose to the Defense Nuclear Agency what field observation and field demonstration studies we think will have merit; conduct those studies after they are approved and revised by DNA; and then follow up with evaluation to find out whether or not the effect is short-range for the tour that was affected or if policies can be implemented long-range at the field sites.

PSYCHOLOGICAL DETERRENTS TO NUCLEAR THEFT

Clare Goodman and George Lapinsky
National Bureau of Standards, Washington, DC 20234

INTRODUCTION

The National Bureau of Standards is presently involved in reviewing research on the topic of psychological deterrents to theft from nuclear facilities. The purpose of this study is to provide a basis for exploratory research programs to expand and improve psychological deterrence elements as an adjunct to conventional physical security systems. A part of this effort has involved expanding upon the preliminary unclassified literature review prepared by Patrick Meguire and Joel Kramer (NBSIR 76-1007).

Literature was searched from a wide variety of disciplines, so that we could consider many possible types of psychological deterrents. The following literature searches were utilized as information sources:

National Criminal Justice Reference Service (NCJRS)
Psychological Abstracts
National Technical Information Service (NTIS)
Ergonomics Abstracts
Social Science Citation Index
Sociological Abstracts
Defense Documentation Center (DDC)
(a) Unclassified
(b) Classified

We have completed the search and received all relevant materials for the above data bases except for the classified DDC search which will be made available to us from DNA in the near future.

In view of the expanding areas of interest at DNA, a broader definition of psychological deterrents is assumed than the one utilized in the Meguire's and Kramer's preliminary literature review. Their review was limited to those deterrents which provided impact on site and which were primarily oriented toward the human senses. For the purposes of this study, a psychological deterrent shall be defined as anything perceived by a potential perpetrator of a nuclear theft as lowering the probability of successfully attaining his or her goal (goal, here, may refer to something other than the theft of a nuclear weapon, such as publicity, embarrassment of government authorities, fulfillment of suicidal fantasy, and a multitude of other rational and irrational goals). The key work in this definition is "perceived"--unless a deterrent is communicated to a potential intruder as a relevant and credible threat to his or her success, it remains outside the realm of psychological deterrence. This definition encompasses not only the immediate physical environment of the intrusion attempt, but also the psychological environment which is thought to precede such an event.

The objective of this paper is to summarize a few of our findings that are to be presented in the final report which is scheduled to be ready for publication at the end of September. There is not enough time to present findings from all types of deterrents that we are researching, therefore the following were selected as a representative sample:

1. Strenuous physical exercise,
2. Noise and vibration,
3. Electromagnetic radiation, and
4. Temperature.

STRENUOUS PHYSICAL EXERCISE

In addition to the effects of exercise mentioned by Meguire and Kramer in the preliminary review, there are a few other specific effects worth noting.

Probably the most relevant to the subject of deterrents to theft is a study done by Wayne Evans (1966) for the U.S. Army in which he examined the effects of fatigue on pistol firing. Evans concluded that heavy exercise did not affect accuracy but did affect time-to-fire. Evans explained, "The pistol firing task seems inherently to require accuracy. Thus, any disability suffered by the subject due to heavy work was not allowed to affect his accuracy but was reflected in an increased aiming time." A somewhat similar finding has been reported for rifle firing with gloves or gas masks used as impediments to performance (Gruber et al., 1965). This also suggests that pistol firing and rifle firing are affected similarly by stress.

That fatigue slows down physical movement patterns seems simple and commonsense, however, research such as that done by Bates, Osternig, and James (1977) at the University of Oregon suggests that the physical slowdown of body movements is not a uniform reduction of the total pattern but rather a dynamic change of the relationships of the body parts involved in the movement. This concept could be very important in optimizing the design of physical and psychological deterrents, and stop-action film analysis of relevant body movements should be considered in both the pre-design and prototype phases if possible. Physical exercise also increases response time to visual and auditory cues (Szmodis, 1977), another design consideration.

Gunnar Borg (1974) in a review of the psychological aspects of physical activities offers several suggestions which may be relevant to security designs: (1) the relationship between subjective and objective work load intensities is such that equal intensity increases in work load over time will be perceived as being much greater than equal; (2) perceived exertion for arm work is greater than for equal intensity leg work; and (3) the function most sensitive to physical stress seems to be hand-arm steadiness.

Cerretelli (1974) in an article concerning endurance, reminds us that psychological factors cannot increase the maximal power of an individual, but they can postpone the onset of fatigue. Thus, intense physical obstacles may be more effective than moderately difficult endurance-type obstacles. In a novel but somewhat related article, Morgan (1971) attempted to affect the physical and psychological difficulty of a submaximal ergometer task by the use of hynotic suggestion. He found that through hypnosis moderate work loads could be made physically and psychologically more difficult, but could not be made less difficult. One may conclude, then, that a physical security system with a physical exertion component should be designed to ensure maximum physical exertion of the target population.

NOISE AND VIBRATION

Despite hundreds of studies that have been conducted, the influence of noise on human responses is still unclear. Meguire and Kramer listed five means by which noise might be an effective deterrent. Basically the following still remain the same.

- Noise may act as an audible alarm for the security guards,
- Noise may be used to warn intruders that their presence has been detected,
- Noise may produce interference or masking of verbal communications between members of an assault team,
- Noise may induce incapacitating physiological effects such as pain, dizziness, blurred vision, nausea, etc., and

o Noise may have negative effects upon intruder intellectual and motor performance, hence slowing the completion of the attack.

After reviewing several studies it became evident that human behavior is rather resistant to short-term noise. Moderately intense noise, although distressing, does not usually impair performance unless the task is an extremely difficult one. Under some circumstances, though, adverse effects do occur, such as when noise masks auditory information, or a temporary hearing loss reduces an individual's ability to receive messages.

Vibration can induce a variety of effects on the body, depending on the intensity characteristics, that is the frequency and displacement, of the vibration. According to Guignard (1972) changes in heart action, respiration, and circulating stress hormones have been observed in response to whole-body vibration. Hasan (1970) states that an "inhibition" of tendon reflexes and the regulation of posture is disturbed.

For most tasks, the intruder will need to take in visual information. The biomechanical influence of vibration can reduce efficiency by interfering with visual input, such as affecting the ability to make precise control adjustments. This was confirmed in a study by Drazin (1976) which showed that at 2 to 4 Hz impairment of vision was particularly evident, but it should be noted that at higher Hz levels impairment was not as large. Cohen (1977) also observed performance impairment occurred when subjects were exposed to a mixture of two different vibration intensities.

Within the reports reviewed on vibration several tolerance limits were mentioned. Three interesting examples were:

1. At approximately 10-14 Hz the ability of the spine to cope with sudden accelerations was affected,
2. At about 20 Hz the head begins to resonate with respect to the body, and
3. Slow wave vibration of approximately .15 Hz to .30 Hz causes motion sickness symptoms in some subjects.

In addition to the physical effects mentioned above, there is some evidence that perceptual distortion of body position takes place when vertical oscillations of 0.1 to 0.5 Hz are used--almost 50% of the subjects in one experiment perceived their position to be 90° out of phase with their true position (Malcolm, 1971 in Reason and Brand, 1975). This could be especially effective in an environment devoid of visual cues.

Finally, two studies completed by Grether et al. (1975) are of particular interest. When heat, noise, and vibration were introduced singly and in various combinations, the results suggested that the combined stress condition`produced less of an effect on performance than the individual stressors. The greatest impairment of performance resulted from the vibration stimulus alone.

RADIATION

The update provided little new information concerning the use of corpuscular and electromagnetic radiations. The most relevant findings were those concerning microwave radiation. Grinbarg and Sheyvekhman (1975), in a review done by NASA, are cited as having reported a raising of sensory thresholds (specifically pain and audition) as an effect of short-term exposure (5 min) to radio-frequency energy fields. The proposed mechanism of this and other perceptual and behavioral effects is the heating and/or ionizing of neural cells. A subjective awareness of warmth was also reported; however, Michaelson (1975) has implied that a microwave field can be created in which peripheral nervous tissue is heated while nearby muscle and skin show no temperature rise. Once the peripheral nerves are heated above some unspecified minimum level, they may begin to fire spontaneously and cause perceptual and behavioral aberrations to occur. It is not known whether these effects can be generated quickly and reliably, without risking permanent damage to the nervous system.

TEMPERATURE

Meguire and Kramer discussed several effective ways temperature may be used as a deterrent. Little additional information on performance degradation and physiological tolerance is available from the literature except for the following studies.

Cold

Cold, in combination with wind and rain, may present a much greater danger to exposed persons than a dry-cold environment. In a dry-cold environment, protection may be obtained by clothing. In a wet-cold environment ones insulation diminishes as air in the clothes is replaced by water which has much higher heat conduction capacity.

Clinically speaking, the so-called wet-cold syndrome is characterized by a very sudden onset of extreme fatigue, fatigue which is out of proportion to the actual physical strain and which can be completely disabling in one-half hour or less. Cognitive processes do not seem to be involved until the onset of general hypothermia.

Several experiments on the effect of cooling the hands, reported that performance on several tasks involving manual dexterity including emergency egress decreased with lowered finger surface temperatures (Lockhart, 1975 and Allan, 1974).

Heat

The amount of time a person can tolerate a hot environment depends on many variables. Generally people who feel uncomfortably hot do not function at maximum efficiency.

Mechanisms exist in the body to contain the core temperature within certain limits. When conditions are severe, the physiological regulations of the body may fail and one faces heat cramps, heat exhaustion, and heat stroke. Heat collapse generally occurs when the body temperature is about 40°C.

An experiment by Wilkerson et al. (1974) demonstrated a connection between body temperature and performance on standard performance tests. With increased temperature the number of vigilance "signals" the subject detected on a vigilance task was improved, but his accuracy in a more complex adding test was deteriorated.

As I mentioned before this paper discusses only a few of the psychological deterrents considered. The following deterrents may also be discussed in the final report:

- Intelligence
- Information management
- Training and selection of personnel
- Intruder characteristics and profiles
- Community relations
- Stress
- Time of day and seasonal effects, and
- Environmental cues.

References

Strenuous Physical Exercise

Bates, B. T., Osternig, L. R., and James, S. L., Fatigue Effects in Running. *Journal of Motor Behavior*, 1977, *9* (3), 203-207.

Borg, G., Psychological Aspects of Physical Activities, in L. A. Larson, (ed.), *Fitness, Health, and Work Capacity*. New York: MacMillan Pub., 1974.

Cerretelli, P., Exercise and Endurance, in L. A. Larson (Ed.), *Fitness, Health, and Work Capacity*. New York: MacMillan Publ, 1974.

Evans, W., Performance on a Skilled Task After Physical Work or in a High Altitude Environment. *Perceptual & Motor Skills*, 1966, *22*, 371-380.

Gruber, A., Dunlap, J. W., DeNittis, G., Sanders, J. L., Perry, V. and Dixon, B. D., *Development of a Methodology for Measuring Infantry Performance in Rifle Firing and Reloading*. Ft. Lee, VA: USATECOM Proj. #8-3-7700-01, Phase II, 1965.

Morgan, W. P., Raven, P. B., Drinkwater, B. L., and Horvath, S. M., *Perceptual and Metabolic Responsivity to Standard Bicycle Ergonometry Following Various Hypnotic Suggestions*. Arlington, VA: Air Force of Scientific Research, April 1971 (NTIS No. AD-767447).

Szmodis, I., Exercise Effects on the Time of Reactions to Auditory Stimuli. *European Journal of Applied Physiology*, 1977, 37, 39-46.

Noise and Vibration

Cohen, H. H., Wasserman, D. E., and Hornuug, R. W., Human Performance and Transmissibility under Sinusoidal and Mixed Vertical Vibration. *Ergonomics*, 1977, *20* (3) 207-216.

Drazin, D. G., Factors affecting vision during vibration. Cited in Kraiss and Moraal (Eds.), *Introduction to Human Engineering*. Verlag TUV Rheinland GmbH, Bonn, Germany, 1976 (p. 235).

Grether, W. F., Harris, C. S., Mohr, G. C., Nixon, C. W., Ohlbaum, M., Sommer, H. C., Thaler, V. H., Veghte, J. H., Effects of combined heat, noise, and vibration stress on human performance and physiological functions. *Aerospace Medicine*, 1971, *42* (10), 1092-1097. Cited in *Foundations of Space Biology and Medicine*, Wash., DC: NASA, 1975. (Chapter 9, Noise and Vibration, by von Gierke, Nixon, and Guignard, p. 371.)

Guignard, J. C., Vibration. In J. C. Guignard and P. F. King, *Aeromedical Aspects of Vibration and Noise*. NATO, AGARD-ograph #151, cited in Kraiss, K. F., and Moraal, *Introduction to Human Engineering*, Verlag TUV Rheinland GmbH, Bonn, Germany, 1976 (p. 234).

Hasan, J., Biomedical Aspects of Low-Frequency Vibration. *Work-Environment-Health*, 1970, *6* (1), 19-45.

Malcolm, R., Human Responses to Vestibular Stimulation and Some Implications to the Flight Environment. (Ph.D. Thesis, McGill Univ.). Cited in Reason, J. T. and Brand, J. J., *Motion Sickness*, NY: Academic Press, 1975.

Radiation

Grinbarg, A. G., cited in J. P. Marbarger and P. V. Vasil'yev (Eds.) Foundations of Space Biology and Medicine, Vol. II. Wash., DC: NASA (#NASA-SP-374-Vol-2-BK-2) (in Chapter 10, Radio-frequency and Microwave Energies, Magnetic and Electric Fields by Sol Michaelson, p. 428), 1975.

Michaelson, S. M., Radio-frequency and Microwave Energies, Magnetic and Electric Fields. In J. P. Marbarger, and P. V. Vasil'yev, (Eds.), Foundations of Space Biology and Medicine, Vol. II. Wash., DC: NASA, 1975. (#NASA-SP-374-Vol-2-BK-2).

Sheyvekhman, B. Y., cited in Michaelson, S. M., referenced above.

Temperature

Allan, J. R., Marcus, P., and Saxton, C., Effect of Cold Hands on an Emergency Egress Procedure. Aerospace Medicine, 1974, 45 (5), 479-481.

Lockhart, J. M., Kiess, H. O., and Clegg, T. J., Effect of Rate and Level of Lowered Finger Surface Temperature on Manual Performance. Journal of Applied Psychology, 1975, 60 (1), 106-113.

Vanggaard, L., Physiological Reactions to Wet-Cold. Aviation Space, and Environmental Medicine, 1975, 46 (1), 33-36.

Wilkerson, J. E., Raven, P. E., Bolduan, N. W., and Horvath, S. M., Adaptations in man's adrenal function in response to acute cold stress. Journal of Applied Physiology, 1974, 36 (2), 183-189.

ORGANIZATION AND MISSION OF THE USAF HUMAN RESOURCES LABORATORY

Dr. Jeffrey E. Kantor
U.S. Air Force Human Resources Laboratory
Brooks Air Force Base, TX 78235

I would like to take a little bit of your time to give you a briefing on what our laboratory does. We are probably not well known outside the Air Force, and there are some people who believe we are not well known in the Air Force, either. But we are the primary agency for conducting behavioral research in the U.S. Air Force.

We do a very wide range of research within the Air Force. We do research on people, on the types of jobs that are conducted in the Air Force, on the training for those jobs, and, within the last 5 to 7 yr, we have become very heavily involved in simulation technology.

The primary mission of the Air Force Human Resources Laboratory is to provide exploratory and advanced development research in the areas of selection, motivation, training, retention, education, career development, force composition, and simulation.

There are six different divisions within the laboratory. We are part of Air Force Systems Command, the headquarters of which are located at Andrews Air Force Base. There are six divisions of the laboratory. First is the Personnel Research Division, which is my division and I will talk a little more specifically about what we do later. Also in San Antonio along with the Personnel Research Division is our Computational Sciences Division. They conduct both basic research into statistical techniques and methodologies and also provide extensive computer and statistical support for the rest of the laboratory. The other division in San Antonio at Brooks Air Force Base is the Occupational Research Division. You will be having a briefing from Hank Ruck who is from that division and will explain to you what they do in terms of his research.

Aside from the three divisions located at Brooks (there is also a Headquarters Section), we have an Advanced Systems Division at Wright Patterson Air Force Base. They are charged with the development of advanced systems and the interface of those systems with hardware and weapons system throughout the Air Force. They do extensive development of simulation hardware, live optic research right now, as well as force composition modeling and projections.

The Technical Training Division is at Lowry Air Force Base in Colorado. They do extensive research on training media for technical training throughout the Air Force and the development of advanced types of training systems.

Finally, the Flying Training Division at Williams Air Force Base is charged primarily with research on flying training. They are perhaps the division most extensively involved in simulation techniques right now. They have what are probably the most advanced state-of-the-art simulators. These simulators are basically T-37 or primary jet trainer simulators and are easily convertible. They are driven by a main computer, which has storage capability, through a computer simulation of visual images of scenes of the State of Arizona. You can fly the simulator wherever you want, under whatever kind of conditions you want, and attempt to do things in the simulator you would obviously never try in the aircraft. Those simulators have the capability of being reconfigured, and they are being reconfigured right now to an A-10, an F-16, and F-15 configuration. They will provide all the flying simulation of those weapon systems in the near future.

Primarily, the bulk of our work is done for the Deputy Chief of Staff for Personnel. However, we also do quite a bit of research for Air Training Command, Tactical Air Command, and some of the other main MAJCOMs within the Air Force. There are two ways that we get involved in research. One is called technology-based research which is in-house research in which we develop the concepts ourselves and use our own in-house funding to provide support for those types of projects. The other is through a Request for Personnel Research, or RPR, where other agencies within the Air Force will document a research need which is then submitted through the appropriate channels and eventually gets down to our laboratory. There it is evaluated for technical need and our ability to support the research. If validated, that becomes a part of our program.

We do probably about half our work in-house and about half our work by contract, but that varies across different divisions.

Just to give you a little appreciation for the wide range of areas that we do work in, this is a partial list of our fiscal year 1978 accomplishments, which include projects from configuring a simulator for A-10 simulation, to various types of hardware development for simulators and the development of a ground-based screening system for pilot selection. The screening system has become a very important area in the Air Force because we are now considering going to a specialized pilot-training program where an individual will come in and be immediately selected for either a fighter track or a fighter assignment or a tanker, transporter, or bomber assignment. So we are looking quite extensively at the characteristics that make people effective as fighter pilots versus effective bomber or transport pilots. We hope to do this without having the individual spend any time in the aircraft that he will not eventually be assigned to. We hope to shortcut the selection system by selection of the aircraft assignment before the individual ever actually flies the airplane.

We have also developed an Air Force Vocational Interest Career Exam which we feel will be very useful in helping match the person with the job and improving our retention of personnel within the Air Force.

FROM THE FLOOR: What is a Holographic Monochrome Pancake Window?

DR. KANTOR: That is part of a simulator system which involves combinations of an image to give an infinity focus for the individual flying the simulator. Previously, the lens system was 32 in, in terms of diameter, and involved very heavy glass lenses. The new system reduces the weight of the lens system considerably. Since it is being used on a movable base simulator, you need to reduce the weight of the lens system as much as possible to give the simulator a better fidelity simulation of the movement of the aircraft. It is also a lot cheaper to do. That involves the simulators being used out at Williams Air Force Base.

I would like to talk a little more extensively about the work we do at the Personnel Research Laboratory since that is what I am mainly familiar with. Our main thrust of our research is on selection techniques. In particular, the emphasis is placed on how to reduce attrition throughout the Air Force. We are spending millions of dollars every year on persons who enter the Air Force and then just do not adapt to military life. So we are developing methodologies to pick out those people who are a high risk not to adapt to the system.

We are also looking at the characteristics of those people who are retained for their 4-yr tour versus those people who are early attrition types. In addition, we are looking at the area of utilization of women. For the past several years, this has been a major concern across DOD. One of the more interesting aspects of our program on utilization of women has dealt with the Air Force Female Pilot Program. In 1976, we started training our first group of female pilots, and we have been monitoring that program since that time. Things look like they are going along quite well, but we will continue monitoring that program for the next few years to insure that the attrition rate of women is no different from the attrition rate of male pilots.

I have already discussed the ground-based screening. Another thing we are doing is the computerized enlistment testing. The way a person enters the military right now is to take a paper and pencil test called the ASVAB or Armed Service Vocational Aptitude Battery. It is a fairly long test and we think we can accrue a good bit of time and money saving by adapting this test to a computer-driven mode. Not only would it save time to present the test through a computer terminal, but we can also, as long as we have that technology available to us, make the test into an adaptive form where the individual sits down at a computer terminal and interacts on a real time basis with the computer. The computer will sample the individual's behavior in a much more time-effective manner than we can now do with paper and pencil tests. We have already run a small test program at a local Armed Forces entrance and examining station, and the response to that was very favorable. We are now looking at DOD funding for an extensive project in that area. It is not inconceivable that within 5 to 7 yr, paper and pencil tests for entrance into the Armed Services will be a thing of the past.

The other project which we have done at the Personnel Research Division, which is probably a little more related to the topics talked about here, is that, within the last year, we finished up a 4-yr program on Air Force security police career fields. In 1974, the Inspector General, who was at that point running the Air Force Security Police Program, decided that the attrition rate among first term security police personnel was excessively high. The Air Force Human Resources Laboratory was asked to conduct a research program designed to identify the correlates of attrition and the correlates of successful job performance in the security police career field.

We administered a battery of tests to about 4500 recruits who were in basic training and scheduled to go to security police career fields. This battery included tests of biographic and demographic background variables, interest type variables, and also aptitude variables. We then followed the progression of these people through the end of technical training, security police technical training, and used a criterion of successfully completing training versus being eliminated during training. Then through a series of linear regression analyses we developed a model using aptitude, background, and interest items to predict attrition. We were fairly successful. We were able to correctly identify 94% of the graduates and also identify 22% of the eliminees. We did a small-scale cost analysis and projected a cost savings of about $225,000 a year using that system.

That was the development phase. One of the problems, though, was that there are fairly few eliminees in security police technical training. So we then followed the same group of individuals through one year of on-the-job performance and then looked at their attrition rate as a criterion at the one-year point.

Using the same variables, we validated the model that we had developed using the technical training criterion, but found that a number of things had happened within the security police force that changed the whole structure or composition of the security police force. In particular, in 1975 the Air Force adopted new enlistment standards which were quite a bit more stringent than the earlier ones, and we started receiving a much better or high quality recruit. Also, the Air Force formed the Security Police Quality Improvement Committee and, under Gen. Sadler, they undertook quite a few job enrichment and job improvement programs which proved to be very effective. One of the things we were monitoring during our research program was job satisfaction in the security police career field, which, when we started, was very low, and by the time we finished was very high. As much as we would like to attribute it to our research, that is not really what happened. It seems as if the Security Police Quality Improvement Committee did produce some very substantial gains, both in satisfaction and a reduction of attrition. Attrition in the security police field actually came down from the 60% range to the 20% range during that period. So it was a very tremendous improvement. That was great for the security police but not so great for our research.

We did not have enough eliminees to really cross-validate or cross-apply or model, but we were fairly sure that the model was effective; however, a lot of the problem went away during the course of the research. So the current status of the selection methodology that we developed is kind of up in the air at this point. What we recommended was to continue monitoring the attrition rate. If the attrition rate continues to decrease, do not do anything at all; and if the attrition rate starts to increase again, it might well be a good idea to implement the selection methodology that we developed.

As a summary, I would like to give you an idea of where we are going in our laboratory and some of our future areas of emphasis. One is for simulation of air combat training. Again, we are becoming very concerned that our fighter pilots are perhaps not as combat-effective as we would like to see them. Historically, combat has shown that most fighter pilots are not effective. In fact, 5% of all fighter pilots historically have accounted for 40% of all air combat kills. So 95% of fighter pilots, no matter how well trained they are, are just not effective in combat. So we are looking at ways to improve combat effectiveness.

One way that I am involved is in terms of helping the combat fighter pilot to manage stress levels that are inherent in the air combat mission. Another way is using the simulators at Luke Air Force Base, which is a detachment of our Flying Training Division, to develop techniques and strategies. It is kind of the reverse of what has historically been the way that new air combat techniques have been developed. We think there is a lot of promise in the approach of using the simulators to actually develop the techniques and then trying them out in the operational environment. It certainly saves a lot of fuel.

We are also looking at guides and specifications for maintenance training simulators. The development of simulators for technical training is another area that is receiving quite a bit of emphasis today.

Another area is maintaining flying skills. One of the big problems we are facing in the Air Force is reduction of flying time. The fuel bill for Air Force flying doubled last year. Given the restrictions that DOD has imposed upon us in terms of flying time and the rising cost of fuel, we just cannot fly as much as we used to. We are seeing flight time reductions of well over 25 to 40% in some squadrons. So the question that we are researching right now is, how often does a person actually have to fly to maintain their tactical skill levels.

We are also looking at enlistment aptitude requirements and whether or not the requirements that are presently in effect are the optimal ones for us. We are looking in the future to a declining 18-yr-old population and we are not going to have the selection ratios. We are not going to have the favorable recruiting environment that we do have right now. So we may have to make some tradeoffs in our enlistment aptitude requirements. But we want to make the best possible tradeoffs to ensure that we still maintain the optimal quality mix.

And we are also looking, again, at adaptive testing applications for selection and assignment.

These are some of the areas that we are looking forward to in the future, and I hope this will give you some appreciation for the capability of the Air Force Human Resources Laboratory.

BEHAVIORAL RESEARCH FOR U.S. AIR FORCES--EUROPE

Mr. Hendrick Ruck
U.S. Air Force Human Resources Laboratory
Brooks Air Force Base, TX 78235

I would like to mention that we at HRL have not been associated with the DNA or security research in the past, and it is a new area to us. We have three of our divisions represented at this meeting--Jeff Kantor from Personnel Research, Dr. Joe Yasutake from the Technical Training Division at Lowry, Captain John Edwards, and myself. We are very interested in finding out what is going on in security and seeing if there is any way we can help in terms of research.

As I said, we are not usually involved in security research. Normally the security police have not tapped us with requests for personnel research other than in that attrition project. Security police, though, have problems within the Air Force and several studies have been conducted that were not research studies. We found that there were problems in planning, budgeting, and programming; there were problems in the chain of command in some sense with one program that was being used. The people in Newark thought that their problems were at least as bad as security police problems in the rest of the Air Force, and demonstrated that by showing that the operational readiness inspections were causing a lot of trouble with the security police. They were not passing as many of those inspections as they had hoped.

Based on kind of information, the Air Staff at Kirkland Air Force Base suggested a MAJCOM squadron reorganization test. That is, they asked each of the major air commands to take a look at how they might restructure their organizations to take care of some of the problems that had been highlighted in these studies. There are manpower regulations in the Air Force which, if you follow them, will give you some answers as to whether your reorganization was successful or not. And of course, the traditional staff study is also helpful.

In response to reported difficulties in the management and conduct of security police operations, the United States Air Forces in Europe (USAFE) decided to test a new organizational structure for security police (SP) squadrons. Although the Air Force has regulations controlling the evaluation of organizational change, the USAFE/SP was interested in gathering objective (scientific) data about the effects of the structural change. Specifically, they wanted to measure the effects of reorganization on jobs performed, individual job satisfaction, organizational climate, and unit productivity. The questions asked were:

a) Did jobs actually change as a result of unit reorganization?
b) Did individual job satisfaction increase or decrease as a result of the restructuring?
c) Did organizational climate improve or deteriorate after unit restructuring?
d) Did unit effectiveness/productivity increase or decrease as a result of the reorganization?
e) Did the base population feel better or worse about security as a result of the reorganization? and finally,
f) Should other units be similarly reorganized?

This paper focuses on the development of instrumentation to be used in answering the six questions of interest.

EXPERIMENTAL DESIGN

Since the questions of change were based in relative terms, a time 1 - time 2 design with matched subjects (organizations) was chosen. Four units, two pairs of similar units in terms of mission and location, were chosen for the experiment. One unit of each pair would be reorganized and the other would serve as control. All four units would be measured in the spring of 1979 and again one year later. Note that the four units together employ approximately 2000 airmen, so individual and subgroup measures are expected to be quite powerful. However, at the unit level, we are dealing with a very small sample (two experimental, two control).

SELECTION AND DEVELOPMENT OF INSTRUMENTS

Several different instruments were necessary to answer the questions of interest, since the questions covered different domains of psychological measurement and were focused at different subjects (security and law enforcement airmen, security police officers, base population, SP squadron subunits, and the SP squadron).

Job Measures

The instruments used to measure the effects of unit restructuring on jobs performed within each unit were U.S. Air Force Job Inventories. Two different job inventories were used--one for enlisted personnel, and one for officers. The job inventories were produced by the USAF Occupational Measurement Center for use in the normal survey program. Each job inventory contains a comprehensive list of tasks that may be performed by personnel whose jobs are to be measured. In addition, background items relating to personal identification and duty history are included. The background items were specifically tailored to USAFE's needs for this study. The 2000 or so individuals involved in the four units will each complete a job inventory at time 1, and again at time 2. Data will include the tasks performed by each individual, an index of relative time spent by each individual on each task performed, background of each individual, empirically derived job types, and, ultimately, comparisons across bases across time. These data will be used to evaluate the effects, if any, of organizational restructuring on jobs performed.

Security Police Assessment Package

AFHRL has been doing research for the past several years on job satisfaction and survey approaches to measuring organizational effectiveness. To meet the needs for "soft" criteria in the Security Police project, the products of two streams of research were particularly useful. A Security Police Assessment Package (SPAP) was developed to measure five major areas of unit effectiveness. The first area included in this survey was a job satisfaction inventory which allows the airmen to indicate their satisfaction with different aspects of their jobs. It also includes a section for supervisors to indicate their satisfaction with various facets of their supervisory duties. The items for this inventory were selected from the Occupational Attitude Inventory (OAI) developed by AFHRL. The OAI is a 200 item questionnaire which addresses 35 job related dimensions of satisfaction. Items relating to 18 of these dimensions were selected as being particularly germaine to job satisfaction of security police.

The remaining inventories in the SPAP were selected from the Organizational Assessment Package (OAP) developed by AFHRL to measure contingency model components impacting on organizational effectiveness. Items were selected from the following four inventories in the OAP:

- o Organizational Climate Inventory - The items in this inventory focus more on organizational aspects than on specific job characteristics addressed in the job satisfaction questionnaire;
- o Supervisor Inventory - These items allow the airmen to indicate attitudes toward characteristics of their supervisors;
- o Perceived Productivity Inventory - These items address airmen's perceptions of the output of their work groups such as quantity or quality of work;
- o Job Inventory - These items permit airmen to indicate the extent to which different characteristics are present in their job and also the amount of selected characteristics that they would like in their job.

In addition to the SPAP, a Base Satisfaction Survey was developed. This survey addresses the satisfaction of base personnel with security police services in areas such as personal protection from crime, traffic flow control, and so forth. This survey only examines law enforcement functions of security police. It was found that the development of a survey of the customers of the security functions of the security police was infeasible in the short time allowed in this project. The Base Satisfaction Survey was administered to approximately 200 individuals at each base. The survey administrator, wearing civilian clothes, surveyed people at random on the base in front of public places such as the Base Exchange, recreation center, and so forth.

The SPAP was administered to all Security Police personnel at each of the bases involved. As with the productivity criteria, both the SPAP and the Base Satisfaction Survey will be administered again at the end of one year. In addition to standard comparisons of changes from baseline levels on the various indices, other analyses such as factor analysis to determine if the factors maintain their integrity will be performed on the data.

Security Police Organizational Effectiveness Measures

The measurement of unit effectiveness or productivity is the riskiest of the measures used in this study, since very little has been published in the area. In measuring SP organizational effectiveness, the following restrictions and assumptions were delineated:

- o unit exercises, alerts, and so on were not to be used since the various inspection agencies employ such measures routinely,
- o the range of unit functions from management to law enforcement to security operations would be covered,
- o measures would be made over time on individuals. A single individual on a bad day would not adversely affect the unit's score,
- o measures would be taken by impartial SP personnel,
- o scoring and weighting of measures would not be released to persons making the measurements.

A team of six experienced security police personnel, together with two research psychologists and an occupational analyst, formed the nucleus for the development of the Security Police Organizational Effectiveness Measures (SPOEM). The SPOEM were developed over 12 work days with team members being augmented by subject area experts whenever necessary.

The process model used to develop the SPOEM borrowed heavily from occupational analysis, task analysis, and specialty knowledge test development methods. The steps used in developing the SPOEM were as follows:

1. All functions performed within a SP squadron were delineated. This served several purposes. First, it provided the psychologists with an understanding of the scope of the measurement problem. Second, it forced the SP personnel to consider SP functions independent of unit organization. Third, it provided the beginning of the road map which the group would use in developing the SPOEM.

2. The functions were grouped into seven major areas. This process resulted in an agreed upon outline of the SPOEM.

3. Importance weights for each of the seven areas were assigned by each of the six SP team members and the project officer. The weights were discussed in terms of percent of effectiveness. The total weights of the seven areas was 100. Weights were discussed publicly and an effort to achieve consensus was made. Unfortunately time constraints precluded full consensus; however, substantial agreement was achieved. The purpose of assigning weights was to target the number of effectiveness items to be written in each of the seven areas. This precluded the writing of many items in a less important area due to ease of describing items. It also caused the team to search for additional items in the important areas.

4. It was decided that no more than 200 organizational effectiveness criteria could be measured in a reasonable amount of time at each base. Each of the seven areas was assigned a proportion of the items based on the areas's weight.

5. Types of effectiveness criteria were reviewed. The concepts behind and forms of behaviorally anchored rating scales (BARS), behavioral expectation scales (BES), criterion objectives for training, test items, inspector general (IG) inspection items, and productivity criteria were discussed. The criterion model chosen was an adaptation of the training criterion objective. Generally, effectiveness criteria would include conditions, behaviors, and standards. Furthermore, they would be expressed as a percentage whenever possible.

6. Each of the seven areas were addressed by the group as a whole. Experts in each area were called in when necessary to provide information and guidance. Prior to writing an idea as an effectiveness item, group consensus was achieved on the following: a) the item measured was, indeed, related to SP unit effectiveness, b) the item was not included in another measure, c) the item belonged to the area under discussion, d) the item was unambiguously related to organizational effectiveness, and e) the item was measurable. Ratings and subjective opinions were generally not allowed as criteria, unless the SP personnel felt quite strongly about an area, and there were no other options.

7. Once the SP effectiveness measures were drafted, the whole list of items was reviewed by the team, project officer, and interested headquarters staff members. Approximately 125 SPOEM items remained after this review.

8. The team spent one day at a SP squadron measuring as many of the effectiveness criteria as possible. The pilot test resulted in the rewriting of a small number of items and the deletion of a number, so that 110 remained.

Although the SPOEM was carefully developed so that it is expected to be a comprehensive measure of organizational effectiveness, the scoring of individual items to derive subscores and overall scores for bases measured with the SPOEM is an important research study that is ongoing. This points out a characteristic of the SPOEM that is desirable in terms of objectivity of measurement. That is, the SP personnel who are measuring each unit with SPOEM items do not know how each item is scored, nor do they know how it is weighted. Thus, the measurement of the individual items is expected to be unaffected by potential bias. One additional comment on the scoring of the SPOEM is the feeling of the authors that unit effectiveness must be measured in light of the policymaker's definition of effectiveness. Therefore, scoring of the SPOEM will be derived from Headquarters policymaker's judgment.

Two approaches are being used to measure the policymaker's judgments regarding organizational effectiveness. The approaches are policy capturing and policy specifying. In the former technique, synthetic unit profiles for each of the seven areas will be presented to headquarters personnel who will be asked to rate the effectiveness of each area for each profile. Regression equations will be developed to determine the weights each item within an area should receive to represent, mathematically, the views of headquarters judges regarding the relationship of each item to unit effectiveness for that area. As a result of policy capturing a score for each of the seven areas of the SPOEM can be derived. The overall unit effectiveness measure will be developed using policy specifying. Using policy specifying, models combining the seven areas will be built by psychologists and the output of those models evaluated by USAFE/SP personnel.

In summary, the purpose of this effort is to evaluate the effects of structural reorganization of Security Police Squadrons in Europe. These effects will be measured in a time 1 - time 2 design using both "soft" and "hard" criteria. The soft measures consist of attitudinal surveys that tap security police perceptions concerning job-related satisfaction, organizational climate, supervisors' characteristics, perceived productivity and job characteristics. Also the perceptions of base personnel concerning the effectiveness of security police will be measured. The hard criteria consist of objective items developed to sample the large number of tasks performed by security police. Taken together, the level of performance on these tasks should indicate the effectiveness of a security police squadron. The level of confidence in the use of the attitudinal items is quite high due to the extensive research program AFHRL has had in this area. Perhaps the most exciting part of this research is the innovative application of policy capturing and policy specifying techniques to combine quantitative productivity criteria. The risk in this part of the research is fairly high; however, the expected results will benefit both the Air Force and the state-of-the-art.

MR. WILLIAMS: Jerry Williams, DNA.

What is the static or the dynamic nature of the leadership during this study?

MR. RUCK: Well, I was hoping to skate through that one, sir. We left a list of things we hoped would not happen to the units during this one-year time period. We were told when we went over there that we had control in experimental units. Only two in two, but it is better than no control units. However, we were then told that there would be no control over such things as operational readiness inspections and things like perhaps a commander changing. We did not feel good about that at all. And in fact, what we asked the project officer there to do is to keep a comprehensive diary of the events in each of the four organizations so that we can take a look at perhaps what may have affected the reorganization. We were not involved in putting together the reorganization; that was not our charter. When we were first contacted, we said that should be our charter before we do anything else.

We have been a little bit worried about outside influences. I think we gave them a list of eight, or is it 15 we finally left?

CAPT. EDWARDS: More like 15.

MR. RUCK: We would like to know immediately about events occurring that we would not like to have happen. So we do not have any real control. However, we do have their pledge that they will control the things they can, but there are an awful lot of things that even the headquarters at USAFE cannot control.

One other point--we made a very concerted effort not to reproduce what the inspector general (IG) or the operational readiness inspection does. We told them that our effectiveness measures may in fact have different results than the IG because our assumptions were different than his. We worried about that because we had the fear that somebody, very high, is going to say, look, HRL said this unit is better now and they failed again. All we can say is, we told you that might happen.

Thank you.

BEHAVIORAL IMPACT ON SHIPBOARD SECURITY

Mr. William Stinson
Navy Personnel R&D Center, San Diego, CA 92152

I would like to give you a little background concerning the overall Shipboard Nuclear Weapons Security System. We are providing the human factors support for the Naval Surface Weapons Center in White Oak in regard to this system. This, by the way, is my interpretation as a behavioral research person of the hardware development; so I hope it correlates reasonably well with White Oak's description of what they are doing.

An advanced system for protection of shipboard physical security is being developed by the Naval Sea Systems Command (NAVSEA-6531D) and Naval Surface Weapons Center, White Oak (NSWC/WO, Code N44). This system must be capable of detecting, classifying, and defeating a variety of unconventional threats involving potential penetration of restricted shipboard spaces or external security boundaries. The human element will be a key factor affecting system capabilities and must be given appropriate consideration throughout the development process.

The motivation and behavioral characteristics of potential adversaries must be taken into account in the development of neutralization capabilities. Prediction of typical and "worst case" assault scenarios can contribute to system design specifications providing for baseline response capability with call-up of supplementary forces as needed.

The required characteristics of response forces must be analyzed in terms of selection, training, tactics, and weaponry support (including communication links). Special attention will need to be given to development of methods for maintaining detection vigilance and timely response capabilities under conditions where the opportunity for action against real targets seldom occurs. Built-in training instrumentation should be considered as a means of exercising selected portions of the security system upon command (unscheduled) to test operational readiness and develop reaction skills.

Design specifications should be verified initially in a laboratory test facility (simulated shipboard environment). Volunteer test subjects could simulate adversary and response force actions. Provisions would need to be made for recording test events in a manner facilitating rapid data analysis (possibly involving real-time keyset entry for computer processing). A capability for playback examination of test events via video tape or video disk would be desirable. Consideration should be given to the possibility of modeling adversary and response force scenarios for use in a war game mode. Interaction consoles could be used by participants in attempting to defeat opposing force tactics. A large number of programmed action alternatives would need to be available for electronic call-up and implementation by participants. This would include selection of various weapons, procedures, and deterrent strategies.

The configuration of security system components must be arranged to assure effective reaction against targets within allowable time constraints. The feasibility of automatic disablement of intruders and/or penetration targets should be considered. Fail-safe provisions will be needed to prevent unintentional activation. Detection redundancy may be needed, providing for automatic dual-mode verification of unauthorized access prior to activation of disabling devices. High reliability will be essential to avoid false alarms which could degrade confidence in security system capabilities and adversely affect response force motivation.

OBJECTIVES

Analyses of human behavioral impacts on system design will involve a phased effort with specification of relatively detailed near-term objectives and general outline of future requirements. The program plan will be updated annually.

Phase I

1. Analyze behavioral characteristics of aggressor and response forces.

    a. Develop a behavioral profile applicable to each category or type of likely adversary (foreign agent, radical group, criminal agent, uncontrolled mob, disaffected crew member, etc.). Predict circumstances and motivation factors which might trigger penetration attempts. Describe preventive measures which can demotivate and discourage potential aggressors. Also, describe behavioral traits which should be taken into account in devising counter actions and conducting negotiations for neutralization of adversaries in the event of successful penetration.

    b. Determine screening measures which can be practically applied in selecting effective guard force members. Consider level of intelligence required (as reflected by basic test battery scores), vocational interest, aptitude in relation to detection/classification abilities, performance reliability, and physical condition. Differentiate by job duty categories where appropriate (supervisory, investigative, control console operator, general guard, etc.).

2. Review capabilities and deficiencies of existing guard force. Conduct structured interviews or questionnaire survey involving mix of ships ranging from smallest to largest type. Include consideration of applicable shore facilities. Identify problems related to quantity/quality of security forces, training, selection, readiness, tactics, communications, and weaponry.

3. Determine possible assault scenarios involving representative ships and shore facilities. Categorize assaults by adversary type and threat level. Determine guard force response scenarios related to adversary type, threat level, restricted space affected, and readiness alert status.

4. Provide input to specifications for design of laboratory test facility (shipboard environmental simulation facility). Include provisions for modeling adversary and guard force scenarios. Investigate feasibility of exercising security system components in a war game mode using interactive consoles to permit guard force simulated response against assault scenarios and adversary simulated actions against programmed guard force scenarios. Performance should be monitored at an evaluation console with provisions for computerized analysis of timeliness and effectiveness of participant actions. As an alternative or supplement to simulation techniques, investigate cost-effective methods of conducting exercises using volunteer test subjects for evaluation of security system capabilities. Determine practical approaches to monitoring participant actions and recording test data in a manner facilitating rapid analysis of performance effectiveness.

Phase II

1. Investigate human factors implications of conceptual design alternatives. Provide input to specifications for man-machine configurations applicable to range of shore facilities and ship types.

2. Develop initial draft of test plan for application at laboratory test facility. Outline test approach, instrumentation requirements, logistics support, and quantity/quality of test participants.

3. Update prior phase analysis as needed (adversary/response force behavioral profiles, guard force selection factors, assault/engagement scenarios, etc.).

Phase III

1. Participate in test operations at laboratory simulation facility to evaluate ADM performance effectiveness and identify human factors problems. Provide input to updated security system specifications.

2. Modify and expand laboratory simulation programming as needed.

3. Develop test plan for application in shipboard evaluation of security system.

APPROACH

Initial Phase

1. Establish liaison with key agencies involved in development of physical security systems to obtain relevant background information. Review literature related to human behavioral aspects of system design, operations, and maintenance.

2. Conduct survey of existing security system capabilities and deficiencies. Distribute questionnaire by mail to appropriate mix of ships and shore facilities. Visit typical facilities to conduct structured interviews as supplement to questionnaire survey.

3. Analyze information obtained from all sources in generating adversary and guard force scenarios. Develop functional diagrams or charts depicting sequential events (decisions and actions).

4. Analyze behavioral patterns of adversaries in previous damage and injury incidents as a basis for development of threat profiles. Apply analysis results, together with theoretical behavioral principles, in devising preventive measures and neutralization procedural guides.

5. Review existing personnel selection procedures in relation to skill levels and reliability qualifications projected for operation and maintenance of modernized security system. Estimate crew size allocation based on consideration of projected workloads involved in all aspects of operation and maintenance.

6. Evaluate various design alternatives for laboratory test facility configurations in terms of effectiveness in testing integrated man/system capabilities. Consider layout flexibility in accommodating several different ship types and threat levels. Assess probability of success in collecting, processing, and analyzing test data under conditions where simulated assaults may involve simultaneous actions by several adversary and guard force participants. Estimate simulation facility computer load based on consideration of requirements for handling programmed scenarios, test event interactions, and evaluation processing.

Follow-on Phases

The approach to be followed in accomplishing objectives beyond the initial work phase will be delineated in future yearly update plans.

COORDINATION

Close coordination between human factors analysts and engineering development personnel will be essential in accomplishing overall system design objectives. This will be particularly important for NSWC/WO tasks and related NPRDC effort involving:

1. Analysis of advanced technology applications in upgrading man/system performance capabilities (Technology Assessment Task).

2. Design and utilization of laboratory test facility with provisions for simulation of shipboard environment (Environmental Simulation Task).

3. Simulation modeling of candidate system characteristics and functions, including guard force and adversary interactions (Computer Modeling Task).

BEHAVIORAL MODEL OF SHIPBOARD PHYSICAL SECURITY--CONTRACTOR SUPPORT

Mr. William Stinson
Navy Personnel R&D Center, San Diego, CA 92152

INTRODUCTION

A computerized simulation model of physical security system operations is planned for development by NSWC/WO as part of the overall Shipboard Nuclear Weapons Security (SNWS) development effort. The system model, hereafter referred to as "macromodel," will use an Interdata 7/32 computer with the capability of accepting Fortran, Cobol, and Basic programming languages. The computer will operate with a variety of peripheral units, including a card reader, disk drive, tape drive, line printer, and graphics console. Computer functions will be controlled by the dynamic OS32 MT operating system.

The Navy Personnel Research and Development Center (NPRDC) is developing a behavioral model of shipboard physical security operations which will operate as a compatible module or subroutine of the SNWS macromodel. The behavioral model must logically describe the interactive effects of important variables affecting guard force and adversary performance in a variety of possible scenarios related to different threat types and shipboard operational conditions.

Proper determination of useful variables to be included in the behavioral model will be of major importance to project success. It must be possible to assign quantitative values to the variables of interest and to demonstrate reliable relationships between the variables and objective measures of security system effectiveness.

Candidate variables would include those with measurable impact on guard force or adversary performance. The variables can be categorized for descriptive convenience in various ways such as:

1. Individual factors - Individual attributes such as intelligence, skill, motivation, etc.

2. Facility characteristics - Number/type of protective barriers, detection sensors, surveillance displays, etc.

3. Environmental conditions - Visibility, noise, ventilation, etc.

4. Operational procedures - Frequency and pattern of guard patrols, frequency of testing to verify performance of detection sensors, method of responding to alarms, etc.

5. Work space configuration - Layout of monitor/control stations for performance effectiveness, location of backup guard force stations in relation to shipboard targets, accessibility of guard force weapons, etc.

6. Equipment aids - Communication links, weaponry support, transportation support, etc.

7. Tactics - Disablement of sensors through tampering, insider collaboration, diversionary actions, kidnapping of hostages, etc.

Several of the candidate behavioral variables may be designated elsewhere as "system" variables for use in the macromodel. Close coordination with SNWC/WO will be required in determining the most effective method of integrating behavioral model and macromodel operations. Appropriate partitioning may be needed to allow for operation of the behavioral model in a "stand alone" mode.

SCOPE

This procurement involves a three-phase effort, with each phase requiring approximately two man-years of work over a time period of one calendar year. The first phase involves the development of methodology and design specifications for the behavioral model. The second phase provides for development and testing of a preliminary working model. The final phase involves integration with the macromodel and demonstration of interaction performance effectiveness.

TECHNICAL OVERVIEW

The behavioral simulation model must be oriented toward accomplishing the primary objective of providing a useful, cost effective tool for rapid analysis of the effectiveness of candidate system configurations. The performance capabilities of guard force and adversary elements will significantly affect system success or failure. Thus, human performance characteristics must be modeled in conjunction with macromodel simulation of physical components in predicting overall system effectiveness.

It is anticipated that development costs and subsequent user operational costs will be greatly affected by the number of variables processed by the model. The degree of precision or sensitivity of the behavioral model should be no greater than that projected for physical components of the macromodel. Provisions for user selection of two or more possible modes of operation with substantially different levels of precision would be desirable.

In order for a variable to be useful for modeling purposes, it must be possible to mathematically define a consistent relationship between the variable and an objective measure of security system performance. It must additionally be possible to assign a quantitative value (or range of values) to the variable based on the results of controlled experiments, surveys of expert opinion, or other suitable data sources.

The behavioral model must be capable of simulating engagements involving several different assault/response scenarios applicable to each threat type of concern (terrorist, foreign agent, radical group, criminal agent, disaffected crew member, etc.). The scenario should cover each threat type under different ship operational conditions where applicable (dockside at foreign ports, dockside at U.S. territorial ports, harbor transit, open ocean steaming, etc.). A mix of ships (carrier, cruiser, destroyer, submarine, etc.) must be covered inasmuch as engagement events may vary considerably by ship type.

A capability for user interaction with the model in a gaming mode would be desirable. This would permit user selection of engagement conditions (type of weapons, tools, tactics, etc.) through keyboard entry at interactive consoles. The performance of participants could be monitored at an evaluation console with provisions for computerized analysis of timeliness and effectiveness of participant actions.

TECHNICAL REQUIREMENTS/TASKS

Phase I Tasks - Development of Methodology and Design Specifications

1. Review Related Physical Security Modeling Work. Several physical security models have been developed or proposed for development in recent years under sponsorship of the Defense Nuclear Agency (DNA) and Nuclear Regulatory Commission (NRC). The contractor will review available documentation concerning these models and if necessary visit the

organizations involved in assessing the advantages and limitations of previous government-sponsored modeling work for possible application in accomplishing SNWS objectives.

2. Determine Useful Behavioral Variables. The contractor must identify appropriate variables which can be used in modeling adversary and guard force performance. The quantitative measure for each variable must be indicated, together with the source of input data. The relationship between each variable and some objective measure of system performance must also be indicated. Separate variable lists should be provided for adversary and guard force elements although several types of variables may be common to both groups. It is important to consider "insider" adversary characteristics in the determination of required variables.

3. Develop Typical Security Scenarios. The model must function in conjunction with scenarios representing typical assault/response force actions and conditions. The contractor will be expected to develop typical scenarios showing adversary and guard force events for each threat type of concern (terrorist, foreign agent, radical group, criminal agent, disaffected crew member, etc.) under various shipboard operational conditions (dockside at foreign ports, dockside at U.S. territorial ports, harbor transit, open ocean steaming, etc.). Provide functional diagrams or charts depicting sequential events (decisions and actions).

4. Develop Model Specifications. The contractor shall develop specifications providing for construction and validation of an effective behavioral model of security system performance. Design provisions shall cover at least the following requirements:

a. Identification of useful behavioral variables, including sources of input data. Describe relationship between each variable and some objective measure of system performance. Describe interaction with macromodel variables where applicable.

b. Determination of computer support requirements. Estimate number of programming instructions required for model implementation. Determine computer memory core requirements. Identify associated peripheral equipment requirements.

c. Description of alternative modeling approaches. Identify at least two candidate modeling configurations with substantially different levels of complexity. This will permit selection of the most desirable approach based on consideration of tradeoffs involving costs of development and operation, operational effectiveness, adaptability, etc.

d. Description of test procedures for verification of model effectiveness. Provide outline of evaluation criteria and procedures for verifying performance effectiveness. Determine method of exercising model in "stand alone" mode prior to interaction with macromodel. Identify any special instrumentation requirements. Detailed test plan will be developed in a later phase of the behavioral modeling effort.

e. Estimation of model costs. Provide estimate of costs involved in development and operation of alternative model configurations. Include all phases of development. Identify manpower requirements for continuing support of model operations.

Phase II Tasks - Development and Testing of Preliminary Working Model

1. Develop algorithms describing relationships between behavioral variables and objective measures of security system effectiveness. Provide for interaction with macromodel variables where applicable. Alternative

modeling approaches proposed by the contractor during the Phase I effort will be reviewed by the Navy, providing the basis for selection of the most appropriate approach for implementation in developing a working model.

2. Develop software programs to exercise model in "stand alone" mode and in conjunction with macromodel. Accomplish debugging as needed. Provide user manual with description of programs and operational procedures.

3. Develop initial data base for behavioral variables. Provide data base management guide with list of behavioral variables and input data sources. Describe methodology applied in generating the data base. Discuss procedures for future upgrading.

4. Prepare test plan for evaluation of model performance effectiveness. Conduct tests to demonstrate capabilities of model in typical scenarios involving the various threat types of concern (terrorist, foreign agent, radical group, criminal agent, disaffected crew member, etc.). Separate test phases may be required to permit initial evaluation of model operations in "stand alone" mode followed by integrated operations with the macromodel.

5. Provide report of test operations and results. Determine required modifications in software or peripheral equipment to meet performance objectives. Estimate cost of modifications. Implementation of modifications and final evaluation of performance effectiveness will be accomplished in subsequent phase of behavioral modeling effort.

Phase III Tasks - Development and Testing of Final Integrated Model Configuration

1. Modify the preliminary working model to upgrade capabilities as needed in meeting performance objectives. Modifications proposed during the Phase II effort will be reviewed by the Navy for selection of the most appropriate approach for implementation by the contractor in developing the final model configuration.

2. Prepare test plan and conduct tests to verify adequacy of model improvements. Correct any remaining problems and repeat tests as needed to demonstrate satisfactory interaction with the macromodel in achieving performance objectives of the integrated final model configuration. Provide report of test operations and results.

3. Revise documentation generated during Phase II effort or develop new documentation to reflect final model requirements, including:

a. Operational procedures manual. Provide a description of model characteristics and implementation procedures, including coverage of associated peripheral equipment. Include orientation concerning macromodel characteristics.

b. Data base management guide. Provide a list of behavioral variables and input data sources. Describe methodology for further upgrading the data base in the future as needed.

c. Programming users manual. Provide a detailed description of programs used with the behavioral model to facilitate future updating and validation as needed.

Following are the guard force performance factors that we would like a contractor to at least consider in modeling: we want to look at anything that affects or has a measurable effect on guard force performance, and that would include individual attributes such as motivation, intelligence level, training, and so forth; operational procedures, organizational structure--that is, how many guards are available in the immediate primary force; work space configuration, environmental conditions--that is, how is performance affected by visibility, noise, anything that has an important effect on performance; and the type of equipment aids that are available to the guard in terms of weapons, communication, and so forth.

Similarly, in modeling the adversary, about the same type of factors need to be taken into account: tactics, target facility layout, individual attributes, organizational structure, environmental conditions, equipment aids, assault objective--whether it is theft or sabotage--and the adversary's knowledge of the security system characteristics.

The type of system technical performance factors that we will need to integrate with are: physical barriers, detection sensors, access control stations, target facility layout, environmental conditions, work space configuration, automatic disablement devices, display monitoring stations, and command/control aids.

That essentially covers our effort that we are getting into. The exact manner in which this model will work will be, of course, the primary determination of the initial phase of effort by the contractor.

MEASURES OF EFFECTIVENESS FOR SHIPBOARD SECURITY

Mr. John Evans
The BDM Corporation, McLean, VA 22102

I have an announcement that BDM has been contracted by the Naval Surface Weapons Center, White Oak, to do a program to derive measures of effectiveness for shipboard nuclear weapons physical security systems. The reason this is in the form of an announcement is because the contract was just awarded, and we are just getting started on it. I did, however, want to make the audience here aware of the fact that this program has been started. It is not a behavioral science program. However, we are interested in finding out what is going on in the field; for instance, Mr. Stinson just mentioned a few items that can be cranked in to the measures of effectiveness formula.

I would like to devote any of the remaining time to Jack Haben, who is representing the Naval Surface Weapons Center here today.

MEASURES OF EFFECTIVENESS FOR SHIPBOARD SECURITY

Mr. John F. Haben
Naval Surface Weapons Center, Silver Spring, MD 20901

Dr. Madden, who is the head of the Shipboard Weapons Security Office, will be here with us tomorrow; I am the deputy. What I would like to say about the measures effectiveness contract is that we consider this so important. It will be a macroscopic look at measures of effectiveness for shipboard security. We have awarded parallel contracts to two contractors, of which Mr. Evans is one. The time span of performance will be roughly the same.

The measures of effectiveness is for the total, overall system. It is a macromodel--we are not looking at specific individual portions, but the total, overall look. That makes the problem interesting but difficult.

OF ANALOGOUS INCIDENTS IN CHARACTERIZING SAFEGUARD THREATS

Mr. Richard S. Schechter
Lawrence Livermore National Laboratories, Livermore, CA 94550
and
Prof. John M. Heineke
University of Santa Clara, Santa Clara, CA 95050

The subject of this presentation is the insider threat to nuclear facilities. Our work is being done for the Lawrence Livermore National Laboratory under the sponsorship of the U.S. Nuclear Regulatory Commission (NRC), and involves two basic objectives. The first is to identify and evaluate potential threats to the security of nuclear facilities posed by insiders. Our focus is primarily on commercial facilities which are licensed by the NRC. Because of the lack of a substantive data base on security incidents at such facilities, we have employed the following two methods in this study. The first is the collection and analysis of data from U.S. industries which have internal security problems analogous to those of the nuclear industry. The second is the interviewing of experts on business and industrial security.

In the first method, we used information collected from three data sets. We collected a data set of major cases of bank fraud and embezzlement (BF&E) from the Federal Deposit Insurance Corporation (FDIC). This is the one data set which we analyzed in detail, and I will present the results of this analysis shortly. We have also collected data on computer-related crime from the data bank at SRI International. Further, we have collected data on drug thefts from manufacturers and distributors, including losses in transit, from the Drug Enforcement Administration.

In addition, we have conducted interviews with high-ranking security officials in a wide variety of Federal agencies and private industries:

1. FDIC Intelligence Section
2. SEC Investigations Department
3. Electronics manufacturing firm
4. Major department store chain
5. Inspector General's Office
6. NASA Research Center
7. Aerospace/Defense Contractor
8. DOE Research Laboratory
9. Bob Curtis, Security Consultant

The internal security problems faced by the source industries examined in this study are in many ways analogous to those of the nuclear industry. To begin with, potential adversaries to the nuclear industry may share common motives with adversaries in the source industries. Some of these motives might include monetary gain, either for personal advancement or out of financial desperation; revenge against an employer for genuine or perceived grievances; intellectual game-playing, including the challenge of pulling off a "caper"; and finally, manipulation by outsiders, either through bribery, coercion, or extortion.

The analogy is also strengthened by common security objectives of the source industries and the nuclear industry. These include protecting vital assets against insider theft, protecting physical facilities against insider sabotage, preventing conspiracy formation, formulating adequate controls and procedures for handling of vital assets and/or information; and protecting the integrity of the accounting system against both deliberate falsification and inadvertent error.

Table 1 presents a breakdown of major cases of bank fraud and embezzlement (BF&E) by the position of the highest ranking insider involved in the case, and table 2 presents a breakdown of these cases on the basis of group size. These analyses were done on a sample of 880 cases of bank fraud and embezzlement of $10,000 or more for the years 1973 to 1977. These major cases account for only 9% of the total number of BF&E incidents, but they account for 53% of the total dollar losses over that time period.

The highest rank in table 1 includes presidents and directors. The next highest rank is high management, which includes senior vice presidents as well as head cashiers. In low/middle management we have branch managers and head tellers. The fourth class consists of non-management staff employees.

Some of the results of this analysis were quite surprising to us. In particular, we were interested in the fact that fully 32% of the cases can be attributed to the most trusted people in the banking industry, the presidents and directors. You will also notice that the mean loss size per case for this category is far higher than for any other category. For these reasons, the top insiders are considered the most severe security threat to the banking industry.

Table 1 also indicates the mean period of concealment for each category. Note that there are no major differences between the first three categories, although staff members are far less successful at concealing their crimes than the management level personnel.

Table 2 summarizes BF&E conspiracies by group size. Roughly 22% of the major cases involved collusion between two or more bank employees. The largest case involved a bank in California in which the president and 15 employees embezzled a half million dollars.

Table 1. Breakdown of BF&E cases of over $10K, by position of highest ranking insider involved in case.*

Rank	Percent cases	Mean loss per case	Period concealed
Pres. or Dir.	32	$244K	19.2 mo.
High Mgmt.	11	$138K	18.9 mo.
L./M. Mgmt.	44	$157K	20.9 mo.
Staff	13	$ 90K	7.9 mo.

Table 2. Conspiracies by insiders--distribution of group size.*

No. in group	No. of cases
1	679
2	130
3	43
4	15
5	5
6-10	6
11-15	1
16-20	1

*Source - FDIC

Table 3 presents some statistics comparing collusion cases with non-collusion cases. The mean size of loss for the collusion cases is about 80% higher than for those which did not involve collusion. The mean time concealed is about 40% higher for those cases with collusion.

Table 4 presents a breakdown of the probability of collusion, given the position of the highest ranking perpetrator involved in the incident. Again, you can see why the top level insider is considered the gravest threat to banking security. Given that the president or director is involved in an incident, there is a 44% chance that at least one other insider is also involved. Note that cases which include only non-management staff members have only an 8% chance of involving collusion.

The results of a statistical analysis of deterrence measures to bank fraud and embezzlement show that the incidence of this type of crime is lower in States with a high frequency of bank examinations, as well as in States which have high banking salaries relative to the average salary for the State. This analysis is based on all BF&E cases in 1975 regardless of size.

I will now discuss some of our findings from interviews with experts on industrial security. We have obtained insight into fundamental problems of internal security; we have learned some typical bases of conspiracy formation; and we have obtained suggestions on options for effective personnel security and operational controls.

The following are some of the fundamental problems of internal security. First of all, there is employee alienation and frustration. This problem is particularly common when employees feel that they have been mistreated. Next, there is the problem of operational convenience being given priority over strict adherence to controls and procedures. For example, many industries require dual controls in which two persons are supposed to witness the proceedings of a complete operation. Sometimes, when people are in a hurry, they will simply ignore these controls and each person will go his own way.

Table 3. Collusion cases vs. non-collusion cases.

	Collusion	No collusion
Mean time of loss	$250,416	$135,724
Mean time concealed	23.72 mo.	26.47 mo.

Table 4. Probability of collusion, given position of highest ranking insider involved in case.

$$P(\text{Collusion}/\text{Pres. or Dir.}) = .44$$

$$P(\text{Collusion}/\text{High Mgmt.}) = .19$$

$$P(\text{Collusion}/\text{L./M. Mgmt.}) = .14$$

$$P(\text{Collusion}/\text{Staff}) = .08$$

Another problem is excessive loyalty to one's immediate supervisor. This appears to be prevalent in the banking industry, which explains why high level executives are so successful in the perpetration of bank fraud and embezzlement. Frequently, a bank will be run as a one-man operation, in which each employee does exactly as he is told, with the manager's indiscretions going unquestioned. Failure to separate and rotate duties is another common shortcoming of internal security. As a result of this failure, one person may be able to carry out all the steps required for a successful theft and coverup.

Conspiracy formation is one of the security issues that is of particular concern to the NRC. In our interviews with security experts, we asked about typical bases of conspiracy formation. One such basis involves an insider who is unwittingly compromised by a fellow employee. This problem again seems prevalent in the banking industry, and can develop as follows: One employee will be asked to circumvent formal procedures for the convenience of a fellow employee. He does not suspect that his friend is really dishonest, so he goes along with the request as a favor. Once he realizes that he has been duped, he is then motivated to participate in the subsequent coverup, so as to hide his own involvement in the affair.

Another common basis of conspiracy formation is mutual friendship coupled with mutual animosity towards the firm. In addition, there is the problem of psychopathic instigators. This is particularly common in the retail industry, where a psychopath will sometimes encourage his co-workers to join in his thievery.

There are also instances in which outsiders manipulate insiders. Sometimes an outsider will target an employee who he feels is especially vulnerable, because he has not received a raise or promotion in a long time and is particularly disgruntled. The outsider will first approach the insider on a very subtle level, without making the slightest suggestion of a theft. He will gain his confidence, and eventually propose an embezzlement as a means of gaining revenge against the employer. Another common method of conspiracy formation involves outsiders intimidating insiders with threats of physical violence.

On the basis of our interviews and data analysis, we would suggest to the NRC a number of options for internal security. First I will discuss the options relating to personnel security. One option is requiring licensees to provide grievance committees for worker complaints, since the disgruntled insider appears to be such a major security problem in a number of different industries. Second, I would stress the team approach to operations, so as to engender a sense of proprietorship among employees. This factor is very beneficial to security, as team members will not hesitate to report illicit activities which they feel are a threat to their team.

Third, I would recommend high wages and benefits for employees. The statistics which I presented on the banking industry demonstrate that this factor does in fact have a deterrence effect on insider theft.

Fourth, I would have new employees sign a list of rules which they can be fired for breaking. Some retail firms use this procedure, which tends to increase employee awareness. Fifth, I would explain methods by which an employee can be compromised by outsiders and fellow employees, as a person armed with this knowledge will be more resistant to such attempts. And sixth, I would require that all employees be treated the same with respect to personnel searches and access requirements, since treating persons differently on the basis of rank can create severe resentment among employees. This type of resentment can be very detrimental to security.

The NRC should also consider a number of options relating to operational controls and procedures. The first recommendation is strict enforcement of separation of duties. This procedure has been recommended in the banking industry to prevent one individual from carrying out all the steps necessary for a successful embezzlement. Second is the rotation of duties on a random basis, when feasible. Forming a conspiracy is very difficult if the adversaries do not know exactly whom they have to incorporate in their attempt on a given day. This procedure is frequently used in guard force assignments.

Third is a mandatory two-week vacation for all employees. This is considered a very effective security measure in the banking industry. A substantial number of BF&E cases which we examined were uncovered while the perpetrator was absent due to vacation, illness, or termination. Apparently, many cases require continuous doctoring of the records to maintain a coverup; as soon as the perpetrator is absent for any length of tire, he can no longer continue that coverup.

Fourth is strict authority limits at all ranks. The high level insider is currently a severe threat to the banking industry because he can often operate with virtually unlimited authority, in lieu of any effective checks and balances. Fifth, I would recommend directly involving NRC officials in physical inventories, using independent sets of records. This procedure would probably be an effective means of preventing coverups by high level management. Finally, I would recommend spontaneous, unannounced audits of the security system by the NRC. The purpose of this measure would be to prevent lax enforcement of security procedures by insiders.

Are there any questions?

FROM THE FLOOR: How much further are you going with this?

MR. SCHECHTER: We intend to analyze our data sets on computer crimes and drug-related thefts. We do not have definite plans for subsequent studies.

FROM THE FLOOR: Are you going to try and tie these three analyses together?

MR. SCHECHTER: We are going to look for similarities between the data sets. So far, there does appear to be one similarity in that the high level insider appears to be a severe threat with respect to computer crime as well as to bank fraud and embezzlement.

FROM THE FLOOR: And when do you think this will be available?

MR. SCHECHTER: It will be available in the first part of 1980. Our effort is part of a broader study which one branch of the NRC is preparing for the Commissioners. That final report will probably be classified, but our portion should be available in a few months.

MR. EVANS: Were there any underlying motives on this embezzlement business, other than getting a lot of money? Was there any reason why they wanted the money or needed the money?

MR. SCHECHTER: That is something which is very difficult to ascertain, as the data files and the case histories do not indicate motives. The persons whom we interviewed seemed to feel that greed is a more important motive than financial desperation.

MR. HARRIS: Concerning the insider problem we talked about the monitoring of how people are behaving, reliability monitoring, and so forth. Do you find that the bankers use a similar method to keep an eye on how people are behaving and so forth?

MR. SCHECHTER: The problem in the banking industry seems to be that there are some people whom nobody watches, and those people are usually the branch managers, the presidents or the directors.

MR. HARRIS: Well, to what extent is that useful in the banking industry? I guess you are saying it is not very.

MR. SCHECHTER: This type of surveillance would probably be effective if it did exist. What some large corporations are now doing is establishing a separate audit branch which is responsible only to those directors who are not officers of the corporation. I think that this type of surveillance could be very effective. If you have an auditor who is directly responsible to the president, I do not think that this would be effective, as he would probably not reveal an attempt involving the president.

MONOMOLECULAR ATMOSPHERIC ION LEVELS

Dr. Charles Wallach
Behavioral Research Associates, Silver Spring, MD 20910

I wish to call the attention of our colleagues to an environmental operator that has been shown to have significant effects on human behavior in areas very relevant to the ergonomics of physical security--particularly the vigilance factor which has been exhaustively scrutinized from nearly every other aspect. This neglected operator is the control of monomolecular atmospheric ion levels in artificial environments. So far as we are aware, ours is the only modern government that has not supported research in this area, although we hope we are wrong and would be most grateful for information on other U.S. workers in this field.

Put simply, the small ions of interest (airions) exist in two polarities, with a +/- baseline ratio of 1.2:1 under natural conditions. This baseline ratio plays a significant part in stabilizing the metabolism of certain active biochemical complexes in the body. It becomes seriously unbalanced by transient effects of electrical fields associated with meteorological phenomena (usually storm cells) and also less transiently by numerous mechanical or structural features of artificial environments.

When these excursions from baseline are large, positive and additive, the behavioral effects manifested by a large proportion of the population are varying degrees of stupor, irrationality and/or hysterical dementia.

That is putting it in strong terms! But although these terms are accurate, please note that the operative words are "varying degrees of." A security guard who goes zombie or maniacal (which does happen at times, according to the Army MP School) can be dealt with quickly and effectively, but in most cases he merely becomes somewhat dull-witted, slower to react, making a false start or two when he does react, gets a bit sleepy or hyperstressed under these conditions while they last. These are the dangerous conditions because they are less obvious, and they occur at hundreds of critical locations with a frequency that might surprise you. They probably account for a large number of otherwise inexplicable failures to react, inappropriate reactions, and accidents with guns, vehicles, etc.

The solution appears simple and cheap; where it is not feasible to change those artificial environmental factors responsible for airionic disbalance which results in the degradation of vigilance, sensory acuity, and reaction time, natural airion balance can be restored naturally by opening windows--or artificially by a properly designed and installed negative-ion generation system.

In response to a question about the cost of negative ion generation equipment in a vigilance-enhancement application, I would like to add that for a single guard position this would be on the order of $100 installed, or a capital investment of less than $20 per man if you figure a 24-hr shift crew complement. In fact it is so cheap this is probably why the subject has been neglected for so long.

I am not selling hardware; I am only trying to call your attention to a concept that needs to be explored, evaluated, made a part of the NBS/SERDS program, and if found as significant as we anticipate it should, be value- and application-engineered for critical structures and vehicles used by security and reaction forces.

I am confident that this will be found of greater practical importance than circadian rhythms (or, perhaps more to the point, ultradian rhythms) on which +/- airion balance and concentrations have overriding effects.

I remain at the service of my colleagues to amplify and explicate the above points, or to explain how electronic positive-ion generation may be used in a adversarial application.

Discussion (Second Day)

PANEL DISCUSSION OF SELECTED PRESENTATIONS

MR. BEASLEY: Good morning, ladies and gentlemen. This morning, we will have Dr. Hall, Dr. Abbott, and Mr. Kramer answer questions regarding their presentations yesterday. These are the three DNA-funded behavioral research efforts that are ongoing at the present time.

In the order of the presentations yesterday, Dr. Hall of Mission Research Corporation presented his performance measurement methodology; Dr. Abbott talked about job selection and training; and Mr. Kramer of NBS talked about vigilance and SERDS.

We added this panel to the agenda because several of you asked me questions concerning these three efforts during and after the presentations yesterday. We wanted to give you a chance to raise those questions this morning.

DR. HEINEKE: Dr. Hall, how was your sample gathered?

DR. HALL: The sample was gathered in the following way. We took our data collection instruments out to the site. Then as people became available, we chose people to be interviewed. We did not use a randomization process in which individuals are randomly selected from the total population of security personnel. It is impractical to randomly select the person who is to be interviewed at a particular point in time because you run into total conflict with the operational procedures. We collected data for all shifts over an 8-d period. We went through a shift change and weekends.

DR. HEINEKE: I see. Neither you nor Dr. Abbott are worried about selection bias in the way those samples were gathered?

DR. HALL: I do not think that is a problem. Because of cost limitations randomization is always a compromise process. As Ward Edwards said, it is nice work if you can get it. It is my opinion that we do not have a serious bias. There are many types of confounding that can occur. One type, of course, is people talking to one another after they have been interviewed. We tried to design our interviews in such a way that the ordering of questions did not create themes.

DR. HEINEKE: Most of the work on the topic indicates that people who volunteer are the ones who obviously have the strongest feelings.

DR. HALL: These samples were not necessarily volunteers. We picked them.

DR. ABBOTT: They were volunteers in the sense that nobody was supposedly told they had to come. At times we interviewed all the people who were available. Bob, I do not know if you ran into this, but particularly on weekends, we just exhausted the available population.

DR. HALL: Well, our interviews lasted about an hour and a half, so each individual had an intensive, extensive interview. That is a lot of data to collect. We really did not run out of people.

DR. ABBOTT: We did on a couple of Sundays and Saturdays when they were low.

DR. HALL: We also interviewed on patrols at the Air Force bases where we did some of the preliminary developments. We actually rode with the patrols and did our interviews while on patrol. We interviewed wherever the people were. In a sense, those people cannot really say, "No, I do not want to talk to you" because you come up with the NCO and he says, "Here is a guy that wants to talk to you." So in a sense, it is not a volunteer situation.

DR. ORTH: It is not a total self-selection process that we used. In other words, we were not waiting at the door for people to come to express their opinions. We went out and got people and said, "Would you come with us?" Then we explained the purpose of the study as you would in any data gathering study, and gave them the opportunity to not volunteer or to volunteer. So it was not just self-selection.

DR. HALL: If they did not want to be interviewed, we tried to talk them into it. If they insisted that they did not want to, we would drop them. For example, new recruits who were preparing for a site inspection may be touchy.

DR. HEINEKE: You asked them questions about whether they used drugs and alcohol, I take it?

DR. HALL: Right.

DR. HEINEKE: Do you believe the answers?

DR. HALL: I think so. For example, we also had the managers' estimate as well as theirs, and in many cases these agree fairly closely. For example, the estimates of the use of marijuana, I think, shows pretty good agreement.

MR. KRAMER: Bob, did you have any feeling that the folks talked with each other about their responses?

DR. HALL: Well, I think there is a certain amount of that. But once again, they were told by us and we tried to get the NCO's to explain to them that this is a confidential thing, their names will not be associated with it in any way. We explained how the data was going to be utilized and that their name would not be associated with the interview data.

I think they tend to be frank. Many of them want to tell you what they think is wrong with the place. Having the time, they have done a lot of thinking about how someone could change things and make them better. In that sense, I think the data are probably good. In the case of drugs, there may be confounding, but I suspect it is minimal.

MR. HANNA: Bob, it might be worthwhile to point out that these people are not asked to discuss their own use of drugs or their own specific capabilities related to their work. They were asked to estimate the involvement of others, in a nondiscriminatory, nonrevelatory sense. There was no potential for self-incrimination. For example, the question might be asked, "What percentage of the guard force do you think smokes pot?"

DR. LEEDY: One of the problems you mentioned yesterday was lack of feedback. Could you explain what you meant?

DR. HALL: We were addressing feedback in terms of performance of their job. "Do you get adequate feedback in terms of your job performance?" This may be an unfair question because you are asking a fairly broad question about a wide array of conditions. However, we did probe that in several areas. We probed it in terms of suggestions such as whether people take their recommendations seriously, or whether they have ever made a recommendation.

It is hard to specify examples of feedback because there is no measurable performance product from which one can receive feedback.

DR. LEEDY: Concerning the series of questions you had about firing of weapons, what evidence is there that the questionnaire response correlates with what would really happen if people got in a situation requiring them to fire their weapons?

DR. HALL: Some correlation is suggested, as is evidenced by firing records. Weapons are fired every 5 or 6 mo. Also, we have the word of the NCO's that most of the people do not know how to use the more complicated heavy weapons, like a recoilless rifle.

DR. LEEDY: Let me restate the question. You asked someone, "Would you shoot your rifle?" He said "Yes" or "No." How much confidence can we have in that kind of response?

DR. HALL: That is a very difficult question to answer. We tried to relate that response to responses on other questions. We asked the question, "What group of people would you not want to team with in the event of a serious attack by an armed group?" We find they would not want to team with approximately one-third of the people.

DR. LEEDY: Do they say why?

DR. HALL: We did not probe that question. However, other answers indicate why. Some of the reasons are: they are inexperienced, they would be likely to shoot somebody, NCO's not trained to lead a coordinated attack. This type of question indicates that one-third of the people might not respond appropriately.

We also asked a similar question in terms of loss of life, "What percent of the force would be willing to risk their life in the event of an armed attack at night?" That came to approximately 54%.

DR. LEEDY: Those who would be willing?

DR. HALL: Yes.

DR. LEEDY: Dr. Abbott, did you ask questions in that general area?

DR. ABBOTT: Yes, we asked about threat and the ability to respond. All I can say, without having analyzed the data thoroughly, is that it appeared to vary from site to site. At one site, we got a very good response. If anything happened, they would work as a team. It was not broken up by platoons. It seemed to be a fairly cohesive company, of which there were very few. In other places, domestically, one I recall particularly, there seemed to be less cohesion, more concern that some would run and not stay and fight.

MR. HABEN: I have some questions for Dr. Hall. In one of your figures, you addressed a question about platoon support, mutual support. You also referred to civilian attitudes which seemed to reinforce isolated feelings. Does this indicate, then, that the security forces are subject to the same "us or them" syndrome to which civilian police forces are subject?

DR. HALL: I do not think it is the same process. I think the security personnel at the base are actually working the undesirable shift. The other people are working the normal eight to five shift. They [security personnel] are doing a job for which there is no product. There is no evidence that they are doing anything, that they are performing any kind of a job. They themselves have no feedback. I think it is the basic nature of the job that has created the problem.

In the police situation, you have an adversary relationship. Security personnel are not catching anybody and they would much rather be in the police role and they would accept it in that sense. So I do not think they are the same thing.

But we found within their platoon a very strong high morale. I think that is a very positive thing which can be used as a motivating factor, providing you have realistic measures of performance on simulated tasks that are reasonable. They will accept simulation provided the simulators are not obviously unrealistic situations.

MR. HABEN: You had another figure which addressed perceived vulnerability. I believe it was approximately 80% who felt that there could be successful penetration. I assume you did not ask about successful engagement after the penetration?

DR. HALL: We did not ask that question. We did probe a bit about attackers being able to attack and get into a structure. Many of the security personnel thought attackers would have difficulty getting out with the nuclear device. We asked a lot of questions in this area: "How could the site be defeated? How would you go about it if you were a terrorist?" We asked a number of questions in this area. And obviously the people on the inside are the ones who know the situation best.

When we asked them about perceived threat, they perceived it to be low, and I think that is realistic. That was from the officers and the enlisted men. But they all agree that if there was a really well-organized attack, the site could be neutralized very effectively.

DR. MULLEN: I have two questions. One, addressed to the entire panel, what does the training consist of for these individuals? I raise that because one of you gentlemen made a statement to the effect that some of these people felt that they were simply a delaying force until the reserves arrived. This harkens back to a lack of confidence in the defensive team there, and the way to instill confidence is to get a well-trained group. Now, you have various things acting upon these people such as shift work. Do they have a training program in which these people operate in teams? You know, like a two-man or a three-man team for defending the site in the event of an attack?

DR. ABBOTT: Yes. Each site has either on-the-job training--and the training "follows" the guards as they are reassigned to new sites--or training before they are assigned to the site itself. So there is training at each site. It tends to differ from site to site depending on the site's specific needs. The people, the graduates from USAMPS, tend to be poorly prepared in weapons, squad tactics, and fire maneuvers. The sites overseas tend to have little ability to train them outside of the site facilities. At both domestic and foreign sites, there are a good number of what they call "conditions," also called "alerts." Some are scheduled for every shift. This is, in a sense, an instruction period where the NCO's and the security people run the guards through scenarios or drills that are as realistic as is feasible. Obviously, how many scenarios can you write for the setting you are in every day? I think this training is reasonably realistic. Dick, I would like to have you comment on its worth.

DR. ORTH: One of the problems we found and addressed was that there were written orders as to where the particular team should deploy under different circumstances. They felt they were holding forces because in their opinion anyone could spot the deployment of their forces during the test. The clear areas were not that far away. So a decently organized terrorist, will go to the site and watch for awhile before planning any moves. In that sense, no matter how much training you have, you know you are going to the place in 1 min, 3 min, 5 min, or whatever the response time is for the particular situation, and the terrorists will be waiting for you. So in that sense it is not a matter of the quality of the training but rather a matter of the quality of the local SOP's.

DR. HALL: Let me say that in our general questions we were not really addressing the details of training. We were asking for their opinion concerning the training at the school. Most of them including the officers and NCO's, and most enlisted personnel below the rank of E4 said it was useless.

DR. MULLEN: Is the school aware of this?

DR. ABBOTT: They are certainly aware of the attitudes because we briefed them on it.

DR. HALL: Most of the enlisted personnel feel that on-the-job training is the best type of training. Many feel it should be conducted out at the site, and not back at the barracks. This may be because they resent training on their own time, off the job.

We have a hunch that some of the best training is done at the platoon level, where NCO's who really take their job seriously do some very clever things. Comments indicate a need for rehearsal and recorded performance data for evaluating their exercises so they themselves could see whether or not they are doing a good job.

DR. MULLEN: My second question is in regard to one of the questions asked these individuals, which was about weapon preference. What were some of the responses?

DR. HALL: What weapons they preferred?

DR. MULLEN: Yes.

DR. HALL: We did not ask them what they preferred. We asked them if they had any equipment that gave them particular problems. That went through everything--weapons, vehicles, what-have-you. Some of the security managers thought that they should do away with the flack vest and the .45 as a side arm. Comments on equipment suggested that security should do away with helmets, and improve gas masks, that the automatic rifle barrel is too long to get out of a pickup quickly and that shotguns should be used when they are guarding structures.

Our main concern with the more complicated weapons is that a lot of people really do not know how to use these weapons. There is no solid evidence that these people can maneuver and deploy the weapons appropriately. I think the Air Force has some concern in this area.

COL. HERRMANN: I think you said that you gathered your data at two [domestic] DARCOM sites and some select sites overseas. I presume the sites were U.S. only, although I am not certain. There is a marked dissimilarity between the DARCOM storage site and the overseas site. Also you have only had a military evaluation. It would be very interesting for you, since you have established a data base for military guards, to broaden your study to include the security forces in an overseas theatre provided by a foreign power, and take a look at their reaction to the guidance that they fulfill, which is basically U.S. guidance. Then also take a look at chemical storage sites that are for the most part guided and directed by civilian personnel.

I think if you would do that, you would certainly have a very interesting comparative analysis of a civilian-guarded site and a military-guarded site, and maybe identify some commonalities and differences. Have you considered it?

DR. ABBOTT: We have hopes to extend that since we have been to five sites overseas. Whether we can get permission to visit NATO sites or those guarded by other countries, I do not know. It certainly would be desirable.

The only way, I think, we can make any comparisons with a comparable civilian force would be to work through NRC. Whether that is comparable, I do not know.

COL. HERRMANN: Well, I think there is comparability. Regulatory guidance, surety guidance, PRP guidance, although not identical, possess a great deal of similarity. Nuclear and chemical sites have a great deal of similarity in the training they require, in their organization, and in the environment in which the guards are working. Although these sites support a different commodity and there is different defense guidance for each commodity, a comparison of these sites might give you an idea about the relative worth of civilian versus military guards.

DR. HALL: I would like to make one comment, Colonel. One of the managers pointed out that the civilian DOD guards at the Army CONUS sites are paid less than a janitor. So the tendency is to come in as a guard and then find some other job in the civil service structure on the post. The attitude of the military security personnel towards these people is that they are not really qualified: they tend to be older and they have serious doubts about whether they could handle the job in a serious situation.

COL. HERRMANN: It is an interesting perception. The upward mobility problem is one that DARCOM has. But by the same token, the [civilian] guards are all ex-military and they are generally all ex-cops, so you have that too.

CAPT. PERKOWSKI: One point on the civilian-military guard interface at the nuclear sites has not been raised. It is that the military police do not see a fulfillment of their expectations to be in law enforcement when they go into physical security. Yet at the two sites that were visited, the civilian DOD guard force has the law enforcement function. The MP's at these sites have purely a nuclear security function. If they speed on post, they get written up by a GS-6 DOD guard in a wrinkled uniform, who, in some cases, gets paid $6,000 a year. And so when you see the civilian-military friction, this must be considered an additional problem.

DR. LEEDY: Dr. Abbott, were the people you interviewed in Europe all military police, 95 Bravo? And did you interview any infantry in the 11 Bravo?

DR. ABBOTT: Ninety-nine percent were 95 Bravo. There were some infantrymen transferred in who had changed MOS's. We did not interview, for instance, the infantry company that was rotated into an European site for 30 d. No.

DR. LEEDY: Okay. That was the question I had.

DR. ORTH: We spoke to two who were outside the 95 Bravo MOS who were serving guard function.

DR. LEEDY: Well, you described the population, I believe, as people who have law enforcement notions. I was wondering whether the particular description you used fit the infantrymen also.

CAPT. PERKOWSKI: We cannot make that comparison any longer because there are no longer infantrymen in a pure security role at the European sites. The corps' artillery sites in Europe now all have security provided by MP companies. They are no longer supported by infantry units, with one exception, and it was not observed. We did visit the corps' storage sites. There also are infantrymen in custodial roles at the non-U.S. sites. The custodial role is differentiated from the security role and we have not really analyzed the custodial roles.

MAJ. BLAKE: I would like to make a comment. Yesterday, when you started your presentations, a lot of us nodded in agreement because these are things we felt we knew. It came to mind that, for all of you, coming in as civilian contractors and working on these problems, there has to be a point when you are learning things that all of us know, yet to you it is new information.

One thing, I recall, is Dr. Abbott saying yesterday that he was surprised at the quality of the MP's guarding nuclear sites. Well, if he had understood the PRP program, he would have realized that those are the best we have. You would not find better soldiers in the entire Army or any place else.

Maybe this comment belongs more to DNA, but once we get a start--and I think that what has been presented here, looking at it from a user's standpoint, is a very good start--it should go a lot further.

Now, what ways do we have to insure that the same contractors or a new contractor would not have to go over the same learning process to get someplace. How do we continue to expand on the knowledge gained at this point and go forward? Because I think we have some very valid uses for what is being gained here.

MR. BEASLEY: Thank you, Maj. Blake, and you too, Col. Herrmann, for leading us into our next subject. We would like to discuss, in the next session, what other things need to be looked at, what other potential performers there are around, accepting that we have recognized these three performers here as a transitional base, if you will. The three were selected from a number of candidate performers that came to the Third Symposia on the Role of Behavioral Science in Physical Security that we had. There are three or four other internationally renowned behavioral science groups that are certainly worthy of a fair consideration. Our deficiency here in DNA, and I think in the entire community of the "people" people in the Services, is that we do not get together frequently, like this, to discuss common needs. I would like to dismiss the panel at this time, bring our DNA people back, and then call on each of you, in round table fashion, to discuss this program element. That is the reason we asked you back today, to discuss what to do with the "Behavioral Phenomenology" program element. What direction should it take, what are the missing pickets on the fence?

What we are looking for is either support for or adverse reaction to the development of a full program element of behavioral phenomenology.

ATTENDEES' ROUND TABLE DISCUSSION: COMMENTS AND OPINIONS ON CURRENT BEHAVIORAL RESEARCH AND FUTURE NEEDS

Those in attendance were invited to comment on areas of behavioral research now being applied to physical security and were asked to suggest new areas of research that could be explored in the future.

Concerning present applied research, several participants felt that there was a need to avoid redundancy in research, a need to "avoid re-inventing the wheel" each time a new contractor came on board. It was suggested that the establishment of an interagency coordinating group might alleviate this problem.

Several of the DNA staff people noted that, in the past, DNA has taken the lead role in initiating behavioral research and that the Armed Services have not generated research proposals for funding by DNA. It was felt that more input from the Services was needed to build a responsive and relevant program of behavioral research.

Various comments reflected the need for more interdisciplinary interaction, especially among human factors engineers, psychologists, and physical security specialists.

Many of those present expressed the opinion that much of the applied behavioral research is not funded because it is presented poorly. Suggestions to remedy this situation were: 1) behavioral scientists should systematically analyze physical security problems from the user's point of view; 2) it should be kept in mind that research should be applicable to organizations with limited resources, since physical security is often given low priority in many agencies; 3) a public relations approach should be used when presenting new research to users; and 4) users must be persuaded to state reasons why past proposals have been turned down so that researchers can be more responsive to the decision-making criteria in the future. In summary, it was felt that behavioral scientists should be more responsive to both the needs and limitations of users, and that users should better communicate their criteria for accepting or rejecting proposals.

Concerning future research, attendees offered many areas of possible research. Most often mentioned was the area of man-machine relationships. A related topic, specific task analysis, was also suggested as an important subject of research. Participants felt that they need to know how personnel interact with their equipment, and exactly what personnel do while on duty (SOP's and formal job descriptions were felt to be helpful, but, in some cases, inadequate).

Another suggestion that attracted popular support was that more research should be done to develop performance criteria and methods of measuring good guard performance. It was felt that good research in this area could have impact on other suggested areas of research such as feedback and reinforcement, development of career structure, motivation, and management style.

Several suggestions were made concerning training. It was felt that the subject of training relevance should be explored. The possibility of integrating training and career development was proposed. Many of the attendees felt that new types of training could be developed to better prepare the guard force; included were: contingency training, error avoidance training, crisis simulation, and especially, more realistic types of training such as gaming. It was felt that such realistic training would also allow behavioral scientists to gather more realistic data under field conditions. Such data could then be used in a systems modelling effort in which researchers could quantitatively describe individual capabilities, site characteristics, equipment capabilities, and probabilities of specific responses.

Suggestions were put forth concerning the fine tuning of the personnel selection process. One participant suggested that the Personnel Reliability Program (PRP) should be reviewed, and revised, if necessary. Another suggested that a correlation of personality variables and guard performance would be useful. Several participants felt that more research was needed on "the insider problem"--that is, how can an organization avoid or recognize employees who may be a security risk?

Also related to personnel issues was the suggestion that an effort should be made to quantify guard capabilities, both physical (strength, endurance, etc.) and mental (sensory thresholds, vigilance capability, stress resistance, etc.) Also mentioned was the need for ergonomic data on possible adversaries (this being suggested as part of a comprehensive threat analysis).

The issue of properly equipping the guard force elicited several comments on the need for equipping personnel with weapons that were relevant to the expected task (i.e., shotguns for bunker guards) and usable (i.e., long-barreled rifles cannot be used easily in a pickup truck).

Finally, a suggestion was made that more research could be done in the area of "guard adjuncts," especially the use of animals as sensing devices, and the use of biofeedback techniques to allow guards to monitor and modify their own internal body states.

After the round table discussion, the participants were briefed on DNA's program element of applied behavioral research and urged to propose research for possible funding in the years 1980 through 1985.

The group then was asked to vote on the issue of petitioning the Physical Security Equipment Action Group (PSEAG) to establish a tri-Services working group that would coordinate and review proposed behavioral research. The vote was affirmative, except for three abstentions.

The participants then voted on the issue of whether a similar symposium on physical security and the role of the behavioral sciences should be held in 1980. The consensus was that there should be a Fifth Annual Symposium and that it be held sometime in the spring of 1980.

LIST OF ATTENDEE'S

Dr. Preston Abbott
Abbott Associates, Inc.
300 N. Washington St.
Alexandria, VA 22314

Mr. Marvin C. Beasley
Defense Nuclear Agency
Attn: SONS
Washington, DC 20305

Ms. Patricia L. Benner
Mission Research Corporation
5503 Cherokee Avenue
Suite 201
Alexandria, VA 22312

Maj. Peter J. Blake
Dept. of Army Personnel
Physical Security
Room 2D-739, Pentagon Bldg.
Washington, DC 20310

Mr. Cezary Bukolt
Naval Material Command
Attn: 046
Room 704, Bldg. CP-5
Washington, DC 20360

Maj. Gen. Richard N. Cody
Defense Nuclear Agency
U.S.A.F. DNA
Washington, DC 20305

Quensel K. Diamond, LCDR USN
Defense Nuclear Agency
Attn: SONS
Washington, DC 20305

Lt. Col. Joseph C. Drauszewski
Defense Nuclear Agency
Attn: SONS
Washington, DC 20305

Cpt. John O. Edwards, Jr.
U.S. Air Force Human Resources Lab.
Force Substainment Section
Force Utilization Branch
Manpower and Personnel Division
Brooks Air Force Base, TX 78235

Mr. John C. Evans
The BDM Corp.
7915 Jones Branch Drive
McLean, VA 22102

Dr. John V. Fechter
Honeywell, Inc. (MN52-3196)
Parkdale Plaza Bldg.
1660 South Highway 100
St. Louis Park, MN 55416
(former employee of the National
Bureau of Standards)

Mr. Angelo C. Giarrantana
Nuclear Regulatory Commission
Division of Safeguard/M.S. 881-SS
Washington, DC 20555

Maj. David H. Gilmore
Defense Logistics Agency
(DLA) TP
Cameron Station
Alexandria, VA 22314

Ms. P. Clare Goodman
National Bureau of Standards
Metrology Bldg., Room A353
Washington, DC 20234

Mr. John M. Haben
Naval Surface Weapons Center
Code N214, Bldg. 405-219
Silver Spring, MD 20901

Dr. Robert J. Hall
Mission Research Corp.
5503 Cherokee Avenue
Suite 201
Alexandria, VA 22312

Mr. Wiley Hall
National Bureau of Standards
Washington, DC 20234

Dr. Larry Harris
Science Applications, Inc.
1200 Prospect Street
La Jolla, CA 92038

Mr. H. Michael Hawkins
Nuclear Regulatory Commission
Division of Safeguard/M.S. 1130-SS
Washington, DC 20555

Dr. J. M. Heineke
J. M. Heineke & Assoc.
12310 Skyline Blvd.
Los Gatos, CA 95030

Dr. J. M. Heineke
Lawrence Livermore Laboratory
P.O. 5504, L/156
Livermore, CA 94550

Ltc. Roger W. Herrmann
U.S. Army Nuclear Chemical Agency
7400 Backlick Rd.
Springfield, VA 22150

Mr. Edgar G. Jacques, II
Naval Surface Weapons Center
Code G-42, Bldg. 4
Room 124
Silver Spring, MD 20901

Mr. Thomas E. (Ted) Johnson
Defense Nuclear Agency
Attn: SONS
Washington, DC 20305

Mr. Harvey B. (Brant) Jones
Nuclear Regulatory Commission
Division of Safeguard/M.S. 881-SS
Washington, DC 20555

Dr. Jeffrey E. Kantor
U.S. Air Force Human Resources
Laboratory
Force Substainment Section
Force Utilization Branch
Manpower & Personnel Division
Brooks Air Force Base, TX 78235

Mr. Arthur A. Klekner
Hdqtrs., Dept. of the Army
U.S. Army Physical Security Branch,
Law Enforcement Division
Washington, DC 20310

Mr. Joel Kramer
National Bureau of Standards
Metrology Bldg., Room A359
Washington, DC 20234

Ltc. Cletus Kuhla
Office of the Secretary for Defense
OUSDRE/Land Warfare, Pentagon
Room 3E-1025
Washington, DC 20301

Mr. George W. Lapinsky, Jr.
National Bureau of Standards
Metrology A353
Washington, DC 20234

Dr. Herbert B. Leedy
U.S. Army Military Personnel Ctr.
DAPC-MST-T
200 Stovall Street
Alexandria, VA 22332

Ltc. Godfrey W. Lepage
U.S. Air Force
Pentagon, Research & Development
Surveillance Division
Room 5C-269
Washington, DC 20330

Dr. Robert Mackie
Human Factors Research
6780 Cortona
Goleta, CA 93017

Dr. Michael Madden
Naval Surface Weapons Center
Code N-44, Bldg. 405-219
Silver Spring, MD 20901

Dr. Stephen T. Margulis
National Bureau of Standards
Building Research, Room A359
Washington, DC 20234

Mr. Tom Midura
Harold Rosenbaum & Associates
40 Mall Road
Suite 207
Burlington, MA 01803

Dr. Robert K. Mullen
Nuclear Regulatory Commission
Division of Safeguard/M.S. 881-SS
Washington, DC 20555

Dr. William Mullen
U.S. Army Human Engineering
Laboratory
Aberdeen Proving Ground
Aberdeen, MD 21005

Mr. Raymond V. Nolan
U.S. Army MERADCOM
Attn: DRXFB-X
Ft. Belvoir, VA 22060

Dr. Richard Orth
Orth Associates
513 West Maple Ave., Suite 205
Vienna, VA 22180

Sgt. Joseph Payne
U.S. Army J. F. Kennedy Center
for Military Assistance
G-3, Special Projects
Ft. Bragg, NC 28307

Cpt. Daniel A. Perkowski
Defense Nuclear Agency
Attn: SONS
Washington, DC 20305

Ms. Ann M. Ramey-Smith
National Bureau of Standards
Metrology Bldg., Room A353
Washington, DC 20234

Donald R. Richards, LTC, USA
Defense Nuclear Agency
Attn: SONS
Washington, DC 20305

Dr. Alexander Rozner
Naval Surface Weapons Center
Code R-32, Bldg. 24-6
Silver Spring, MD 20901

Hendrick W. Ruck
U.S. Air Force Human Resources
Laboratory
Brooks Air Force Base, TX 78235

Mr. Richard S. Schechter
Lawrence Livermore Laboratory
University of California
P.O. Box 808, L-97
Livermore, CA 94550

Ltc. Louis E. Shaw
Headquarters, U.S. Marine Corps
Quantico, VA 22134

Mrs. LaDonna Short
Dept. of the Army, Project Office
for Physical Security Equipment
Commander, USA Mobility Equipment
Research & Development Cmd
Attn: DPRDME-ZPS
Ft. Belvoir, VA 22060

Mr. Robert A. Silano
Mission Research Corp.
5503 Cherokee Avenue
Suite 201
Alexandria, VA 22312

Mr. Andy Smith
U.S. Air Force Weapons Laboratory
AFWL/NSCA
Kirtland Air Force Base, NM 87117

Mr. Daryl K. Solomonson
Mission Research Avenue
Suite 201
Alexandria, VA 22312

Mr. William Stinson
Navy Personnel Research &
Development Center
Code P311
San Diego, CA 92152

Dr. Harold P. Van Cott
National Bureau of Standards
Metrology Bldg., Room A365
Washington, DC 20234

Dr. Charles Wallach
President, Behavioral Research
Associates, Inc.
1220 Blair Mill Road #1205
Silver Spring, MD 20910

Dr. Stein Weissenberger
Lawrence Livermore Laboratory
P.O. Box 5540-L/156
Livermore, CA 94550

Lt. Col. Gerald O. Williams
Defense Nuclear Agency
Attn: SONS
Washington, DC 20305

Mr. Joseph Y. Yasutake
U.S. Air Force Human Resource Lab.
Brooks Air Force Base, TX 78235

NBS-114A (REV. 2-80)

U.S. DEPT. OF COMM.

BIBLIOGRAPHIC DATA SHEET *(See instructions)*

1. PUBLICATION OR REPORT NO.
NBSIR 81-2207(R)

2. Performing Organ. Report No.

3. Publication Date
February 1981

4. TITLE AND SUBTITLE
The Role of Behavioral Science in Physical Security. Proceedings of the Fourth Annual Symposium, July 25-26, 1979

5. AUTHOR(S) Edited by George M. Lapinsky, Ann Ramey-Smith, and Stephen T. Margulis

6. PERFORMING ORGANIZATION *(If joint or other than NBS, see instructions)*

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

7. Contract/Grant No.

8. Type of Report & Period Covered

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS *(Street, City, State, ZIP)*
Nuclear Surety Directorate
Defense Nuclear Agency
Washington, DC 20305

10. SUPPLEMENTARY NOTES

□ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)*

This document contains the proceedings of the fourth annual symposium on "The Role of Behavioral Science in Physical Security," held on July 25-26, 1979. The symposium provided a forum for presenting and discussing current behavioral science contributions to physical security. Generally, attendance was limited to key personnel in the services, other Government Agencies, and private firms currently on contract with the Defense Nuclear Agency. Papers were presented on the first day, followed by a discussion session the second day.

12. KEY WORDS *(Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)*
Behavioral science; collusion; ergonomics; human factors; performance; personnel selection; physical security; psychological deterrents; threat analysis; training; vigilance

13. AVAILABILITY

□ Unlimited
☒ For Official Distribution. Do Not Release to NTIS
□ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
□ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

15. Price

☆U.S. GOVERNMENT PRINTING OFFICE: 1981-340-997/1571

2993